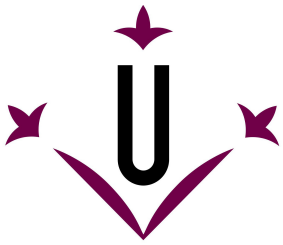
Universitat de Lleida

Privacy-preserving protocols for the e-society

Núria Busom Figueres



Universitat de Lleida

DOCTORAL THESIS

PRIVACY-PRESERVING PROTOCOLS FOR THE e-SOCIETY

Núria Busom Figueres

This thesis is presented for the degree of Doctor from the Universitat de Lleida

Doctoral Programme in Engineering and Information Technology

Advisers:

Dr. Francesc Sebé Feixas

Dr. Magda Valls Marsal

2017

Abstract

The widespread use of mobile phones and other electronic devices is profoundly changing the way in which we communicate. The e-Society is no more a utopia. Nowadays, we can carry out almost any transaction through the Internet: buy products, request official documents, gain access to medical results, among many other things. All these activities imply, though, privacy risks for the citizens.

This thesis focuses on an e-Society sub-branch, e-Services, which covers the entire commerce and consumption of goods through the Internet. There are many types of services, but we will deal with three of them: loyalty systems, smart metering systems and reputation systems.

Loyalty systems are conceived by vendors to win over new customers and encourage old customers to keep buying. Users who follow the fidelity programme receive some kind of reward, usually in the form of a discount or voucher. On the other hand, in order to track customer fidelity, vendors usually keep a record of all sales, including customer name and the list of products they bought. All this personal information is very sensitive and may be used for fraudulent or unauthorized targeted advertising.

Smart metering systems record domestic consumption of electric energy in small intervals of time and communicate this information to the utility. The supplier benefits from this information, since it can adjust the energy production and avoid electricity surplus. On the other hand, the customer gains access to detailed information on her consumption;; hence, she may adapt her consumption habits in order to save on the bill. Nevertheless, anyone who has access to this information would be able to infer personal information such as which appliances are working or even whether there is anyone at home at a given time.

Reputation systems allow users to give their opinion about products they bought or even to evaluate the utility of other users' opinions. This information helps to build up trust reputation. Other users' opinions may help users to make their own decisions. Nevertheless, this information may be used to reveal the preferences of the users who take part actively on such platforms.

This thesis revises privacy problems related to the e-Services mentioned above, studies current bibliography, analyses their weaknesses, and presents new proposals. As a result of this thesis three scientific papers, one in each aforementioned e-Service type, have been published, all focusing on privacy issues and maintaining efficiency and usability.

Kurzfassung

Die weit verbreitete Nutzung von Mobiltelefonen und anderen elektronischen Geräten verändert sich tiefgreifend, die Art wie wir kommunizieren. Die E-Society, elektronische Gesellschaft, ist keine Utopie mehr. Heutzutage können wir fast alle Transaktionen via Internet durchführen: Ware kaufen, amtliche Urkunden anfordern, Zugang zu Befunde erhalten, u. a. All das bedeutet aber, dass die Privatsphäre der Bürger in Gefahr ist.

Diese Dissertation konzentriert sich auf einen Unterbereich der E-Society -die E-Services- der den Handel und den Verbrauch von Waren über das Internet einnimmt. Es gibt viele Sorten von Dienstleistungen, aber wir werden mit drei dieser Arten umgehen: Kundenbindungs- (loyalty systems), intelligente Mess- (smart metering systems) und Reputationssysteme (reputation systems).

Kundenbindungssysteme werden von Anbietern konzipiert, um neue Kunden zu gewinnen und alte Kunden zu ermutigen, weiter zu kaufen. Benutzer, die dem Treueprogramm folgen, erhalten eine Belohnung -normalerweise in Form von Rabatt oder Gutschein. Andererseits, um die Treue der Kunden zu verfolgen, erstellen die Verkäufer normalerweise ein Register über alle Verkäufe, einschließlich der Namen der Kunden und der Liste der Produkte, die sie gekauft haben. Alle diese persönlichen Informationen sind sehr empfindlich und können für betrügerische oder nicht autorisierte gezielte Werbung verwendet werden.

Intelligente Messsysteme erfassen den Hausstromverbrauch in kleinen Zeitintervallen und leiten diese Informationen an den Dienstanbieter weiter. Der Stromversorger profitiert von diesen Informationen, da er die Energieproduktion anpassen und den Stromüberschuss vermeiden kann. Darüber hinaus erhalten die Kunden detaillierte Informationen über ihren Stromverbrauch, daher können sie ihre Konsumgewohnheiten anpassen, um zu sparen. Dennoch könnte jeder, der Zugang zu diesen Informationen hat, daraus schließen, welche Haushaltsgeräte funktionieren und damit wissen ob es irgendjemanden zu Hause gibt.

Reputationssysteme ermöglichen es Benutzern, ihre Meinung über Ware zugeben, die sie gekauft haben, oder sogar die Meinungen anderer Nutzer zu bewerten. Diese Informationen helfen, Vertrauen Reputation aufzubauen. Die Meinungen anderer Nutzer können den Benutzern helfen, ihre eigenen Entscheidungen zu treffen. Dennoch können diese Informationen verwendet werden, um die Präferenzen der Nutzer, die sich aktiv an solchen Plattformen beteiligen, zu zeigen.

In dieser Doktorarbeit werden die Datenschutzprobleme im Zusammenhang mit E-Services untersucht, aktuelle wissenschaftliche Artikel durchgearbeitet, ihre Schwächen analysiert und Lösungsvorschläge dafür gemacht. Als Ergebnis dieser Dissertation wurden drei wissenschaftliche Arbeiten veröffentlicht, eine in jedem o. g. E-Service-Typ. Die drei konzentrieren sich auf Datenschutzfragen, ohne Effizienz und Benutzerfreundlichkeit zu verlieren.

Resum

L'ús de telèfons mòbils i altres dispositius electrònics està conduint la societat cap a una nova manera de comunicar-se. La e-Societat ja no és una utopia. Avui en dia, podem fer gairebé qualsevol tipus de transacció a través d'Internet: comprar productes, sol·licitar documents oficials, accedir a resultats mèdics, entre moltes altres coses. Tot això implica riscos pel que fa a la privadesa dels ciutadans.

Aquesta tesi se centra en una de les subbranques de la e-Societat, els e-Serveis, que abraça tot el comerç i consum de béns a través d'Internet. Hi ha serveis de moltes menes, però ens centrarem en els sistemes de fidelitat (*loyalty systems*), els mesuradors intel·ligents d'electricitat (*smart metering systems*) i els sistemes de reputació (*reputation systems*).

Els sistemes de fidelitat són una eina dels venedors per atraure nous compradors i consolidar els ja antics. Els usuaris que segueixen el programa de fidelitat reben algun tipus de recompensa, normalment en forma de descompte o regal. Per una altra banda, per tal de portar un registre de la fidelitat dels clients, els venedors normalment emmagatzemen molta informació sobre els compradors, com el nom i quins productes han comprat. Tota aquesta informació personal és molt sensible i podria ser emprada fraudulentament i sense autorització per crear perfils d'usuaris en publicitat dirigida.

Els mesuradors intel·ligents capten informació del consum elèctric cada poc temps i l'envien regularment al proveïdor. La companyia elèctrica es beneficia d'aquesta informació ja que pot regular la producció d'electricitat i evitar una sobreproducció. Per una altra banda, el client disposa de tota la informació detallada sobre el seu consum i això li permet adaptar els seus hàbits de consum per tal d'estalviar en la seva factura. Malgrat això, qualsevol que tingui accés a aquesta informació, podria inferir quins electrodomèstics estan funcionant dins d'una casa i, fins i tot, esbrinar si hi ha algú a dins en un moment determinat.

Els sistemes de reputació permeten que els usuaris donin la seva opinió sobre productes que han comprat o, fins i tot, que avaluïn la utilitat de les opinions proporcionades per altres usuaris del sistema. Aquesta informació ajuda a crear una reputació. L'opinió d'altres usuaris pot arribar a ajudar a que algú es decideixi a comprar un producte o no. Tanmateix, aquesta informació també pot ser utilitzada per conèixer les preferències i gustos dels usuaris que participen activament en aquest tipus de plataforma.

Aquesta tesi revisa els problemes de privadesa relacionats amb els e-Serveis abans mencionats, estudia propostes actuals, n'analitza els seus punts febles i fa noves propostes. Com a resultat d'aquesta tesi s'ha realitzat una contribució a cada un dels tres e-Serveis esmentats, tot centrant-se en garantir la seguretat i privadesa de les dades mantenint l'eficiència i la usabilitat.

Resumen

El uso de teléfonos móviles y otros dispositivos electrónicos está llevando la sociedad hacia una nueva manera de comunicarse. La e-Sociedad ya no es una utopía. Hoy en día, podemos hacer casi cualquier tipo de transacción a través de Internet: comprar productos, solicitar documentos oficiales, acceder a resultados médicos, entre otras muchas cosas. Todo ello implica riesgos en cuanto a la privacidad de los ciudadanos.

Esta tesis se centra en una de las subramas de la e-Sociedad, los e-Servicios, que abarca todo el comercio y consumo de bienes a través de Internet. Hay servicios de muchos tipos, pero nos centraremos en los sistemas de fidelidad (*loyalty systems*), los medidores inteligentes de electricidad (*smart metering systems*) y los sistemas de reputación (*reputation systems*).

Los sistemas de fidelidad son una herramienta de los vendedores para atraer nuevos compradores y consolidar los ya antiguos. Los usuarios que siguen el programa de fidelidad reciben algún tipo de recompensa, normalmente en forma de descuento o regalo. Por otra parte, a fin de llevar un registro de la fidelidad de los clientes, los vendedores normalmente almacenan mucha información sobre los compradores, como el nombre y qué productos han comprado. Toda esta información personal es muy sensible y podría ser empleada fraudulentamente y sin autorización para crear perfiles de usuarios en publicidad dirigida.

Los medidores inteligentes captan información del consumo eléctrico cada poco tiempo y la envían regularmente al proveedor. La compañía eléctrica se beneficia de esta información ya que puede regular la producción de electricidad y evitar una sobreproducción. Por otra parte, el cliente dispone de toda la información detallada sobre su consumo y esto le permite adaptar sus hábitos de consumo para ahorrar en su factura. Sin embargo, cualquiera que tenga acceso a esta información, podría inferir qué electrodomésticos están funcionando dentro de una casa e, incluso, averiguar si hay alguien dentro en un momento dado.

Los sistemas de reputación permiten que los usuarios den su opinión sobre productos que han comprado o, incluso, que evalúen la utilidad de las opiniones proporcionadas por otros usuarios del sistema. Esta información ayuda a crear una reputación. La opinión de otros usuarios puede llegar a ayudar a que alguien se decida a comprar un producto o no. Sin embargo, esta información también puede ser utilizada para conocer las preferencias y gustos de los usuarios que participan activamente en este tipo de plataforma.

Esta tesis revisa los problemas de privacidad relacionados con los e-Servicios, estudia propuestas actuales, analiza sus puntos débiles y hace nuevas propuestas. Como resultado de esta tesis se ha realizado una contribución a cada uno de los tres e-Servicios mencionados, centrándose en garantizar la seguridad y privacidad manteniendo la eficiencia y la usabilidad.

Contents

List of Figures

List of Tables

– No oblideu mai que, si ens aixequem ben d'hora, però ben d'hora, ben d'hora, ben d'hora i no hi han retrets, no hi han excuses, i ens posem a pencar... som un país imparable.[a]

Josep Guardiola, when he was given the Medal of Honour at the Catalan Parliament

[a] Never forget that if we wake up early in the morning, very early, with no reproaches to anybody and using no excuses, and we start working hard, we are an unstoppable country.

1 Introduction

This thesis is mainly focused on the analysis and design of some privacy-preserving proposals for e-Services.

This chapter provides an overview of some concepts related to the e-Society, which covers a broad range of areas which have been adapted to the impact of digital technologies. First, a brief introduction to e-Society is given, itemizing some of its main branches. Next, loyalty systems, smart metering systems and reputation systems are introduced, focusing on their main threats to privacy. Finally, the goals of this work are presented, along with the contributions made during the development of this thesis.

1.1 Context

The ubiquity of the Internet and the widespread use of mobile phones, and even wearable technologies, are profoundly changing the way in which we communicate. We increasingly rely on smart gadgets to do daily things as technology becomes fully integrated into our everyday lives. The Internet of Things (IoT), although not a new concept, is currently sky-rocketing. Gartner [Gar17] states that there will be 20.4 billion devices connected to the Internet by 2020, up 41 per cent from the current amount. In 2017, the consumer sector represents 63 per cent of the overall number of applications in use. We are moving towards a new society, where new electronic services are emerging to improve our lives. This is known as electronic Society, or *e-Society* for short.

The term *e-Society* covers a wide range of applications [MLV07] in the following challenging areas:

- *e-Business*: focused on facilitating technologies for the communication between businesses and customers, or between businesses themselves, over the Internet [HR17]. It includes the study of new commercial strategies, models and architectures, payment methods and e-Services, among many others.

e-Services: sub-branch that embraces the entire commerce and consumption of goods, both hedonic and utilitarian, through the Internet. e-Services are gaining in importance since they provide on-demand solutions to customers. However, they deal with sensitive personal data. For this reason, the threat to privacy is very critical. This thesis confronts some open problems that arise in this field.

- *e-Learning*: comprises technologies that permit, either synchronously or asynchronously, interaction between teachers and students, and therefore enhance efficient learning [DC17]. It breaks down time and space barriers and students can learn whenever and wherever they want. For this reason it is really important to track the students' learning process, so that the tutors can be aware of the activities being undertaken and the resources being consumed by the students. At the same time, this tracking infringes on students' privacy.

- *e-Government*: focused on digital interactions between Government and citizens, other governments, employees or companies [FRS17]. It is still in the early stages of development in many countries and jurisdictions. Its goal is to be able to offer a range of public services to citizens in an efficient and cost effective manner, while maintaining privacy.

- *e-Mobility*: intended to fulfil mobility needs by including intelligent devices in vehicles and in traffic management nodes. This allows users to be traffic and parking status aware, it makes their driving safer and more coordinated and it informs about charging infrastructures for electrical vehicles, among many others. The communication between devices permits automatic data collection that can be used to track drivers' behaviour.

- *e-Health*: includes a wide range of digital technologies applied to the health care sector, such as telemedicine, collaborative systems for patient diagnosis or online systems for medical records [VSA+15]. One of the aspects preventing widespread acceptance of the use of e-Health services is the issue of privacy regarding patient health information.

These areas are outlined in Figure 1.1, which offers a non-exhaustive taxonomy of the most important branches and sub-branches of e-Society. This scheme has been obtained by gathering hot topics confronted in the most important current technological congresses and workshops focused on the new threats and challenges that e-Society poses.

Digital society includes an appealing vast environment for academics from all research areas. Both industry and researchers are pushed towards finding new solutions for these new challenging problems. Although this revolutionary transformation of the world has collapsed geographical barriers that once restricted communication, it also poses a threat to user privacy.

Public Key Infrastructures (PKI) facilitate the implementation of secure systems (see Chapter 2), but at the same time security makes things slower and more complex. It is usually said that security is PAIN, which stands for the acronym of its four components: *P*rivacy, *A*uthentication, *I*ntegrity and *N*on-repudiation.

- *Privacy* is defined as "the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed" [Shi00].

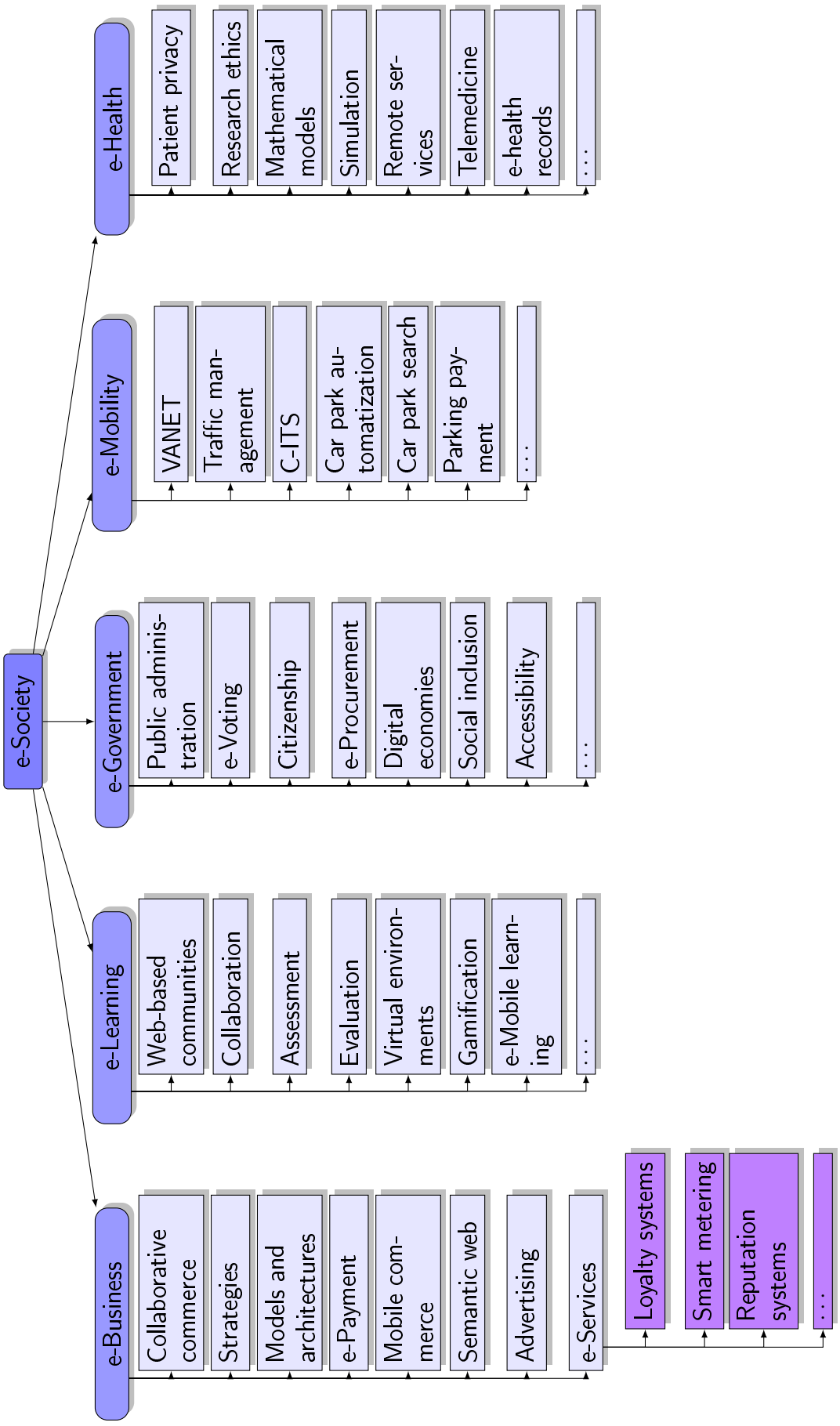


Figure 1.1: Scheme of some important e-Society branches and sub-branches

- *Authentication* is defined as "The process of verifying an identity claimed by or for a system entity". This is fundamental in an electronic transaction to be sure of the identity of the parties involved.
- *Integrity* is defined as "The property that information has not been modified or destroyed in an unauthorized manner".
- *Non-repudiation* is defined as "A security service that provides protection against false denial of involvement in a communication".

If a platform satisfies these properties, its users can be confident that their communications are confidential, unaltered and that they truly occur.

1.2 e-Services

Digital users may use e-Services to remotely carry out actions that until now were reserved for the real world. In order to be successful, these services must be fast, easy-to-use and friendly, but without losing sight of privacy.

Nowadays, there are numerous e-Services platforms, but this thesis is focused on the following three:

Loyalty systems are structured marketing strategies conceived by vendors to boost their sales, by winning over new customers and by encouraging old customers to keep buying. In exchange, customers may receive some kind of reward, such as discounts or coupons.

In order to track customer loyalty, vendors may keep a register of all sales, including customer name and the list of products they bought. Even if vendors do not want to use this information harmfully, this information is very sensitive. It may be infinitely profitable for creating user profiles with their preferences and tendencies and, then, using this information for fraudulent or unauthorized targeted advertising.

Smart metering systems record domestic consumption of electric energy in small intervals of time and communicate this information to the utility for monitoring and billing purposes. With this information, the supplier is able to adjust the energy production and avoid electricity surplus. The customer may benefit from different consumption plans, more accurate billing and better knowledge of consumption habits.

Unfortunately, if an attacker is listening to those consumption readings, she may obtain a great deal of sensitive information, such as which appliances are working or even whether there is anyone at home. She could even infer the users' daily routine. Hence, this behaviour should be prevented.

Reputation systems are platforms that allow users to rate products, vendors or other users in order to build up trust reputation. Other users' opinions may help users to make their own decisions. When rating, users may obtain some kind of reward, such as badges to show off or other commercial advantages.

The history of a user's ratings reveals her preferences, that may in some cases be sensitive information.

1.3 Goals of this thesis

The security challenges tackled in this thesis are focused on the following aspects:

- Study the most suitable cryptographic tools for the needs arising in the design of e-Services protocols confronted in this thesis.
- Analyse existing coupon systems, identify the drawbacks of one of them and design a system that improves its performance.
- Analyse the requirements of a smart metering system, study existing proposals, identify their weaknesses and design a system that fulfils all the requirements identified.
- Study existing reputation systems, both commercial and academic, identify possible attacks against them and design a suitable privacy-preserving reputation system.

1.4 Contributions

The research work carried out during the development of this thesis led to two scientific papers published in first-quartile international journals and one paper presented at a cryptographic security conference.

- N. Busom, F. Sebé, M. Valls, **A publicly verifiable counter-based loyalty system** published in Proceedings of XIV Reunión Española sobre Criptología y Seguridad de la Información [BSV16].
  Abstract: For ages, companies have invested much effort to run successful loyalty programmes to gain and reward loyal customers. Nowadays, most of these programmes are implemented using smart cards or mobile device technologies. Privacy and security requirements are guaranteed by the underlying cryptographic protocol. As opposed to traditional paper-based coupons, in digital systems it might be easy to produce an identical copy of an electronic coupon. Hence these systems must prevent double-spending and ensure privacy. In this paper we present a loyalty system protocol which adds the publicly verifiable property to an existing proposal, while providing better performance.
- N. Busom, R. Petrlic, F. Sebé, C. Sorge, M. Valls, **Efficient smart metering based on homomorphic encryption** published in the Computer Communications journal [BPS+16].
  Abstract: Smart meters send fine-grained client electricity consumption readings to suppliers. Although this presents advantages for both entities, it results in a serious loss of privacy for customers. We present a monitoring-purpose system that preserves customers' privacy by homomorphically aggregating the consumptions of all n members of a neighbourhood. The proposal has an efficient linear O(n) communication cost and is proven to preserve customers' privacy even in the presence of a corrupted substation and some malicious smart meters. It requires neither secure communication channels nor a trusted third party (except for issuing public-key certificates). Computation on the smart meters is limited to modular exponentiations. These favourable properties come at the expense of increased computation cost on the electricity suppliers' side. We show that the computation is easily feasible for realistic parameter choices.

- N. Busom, R. Petrlic, F. Sebé, C. Sorge, M. Valls, **A privacy-preserving reputation system with user rewards** published in Journal of Network and Computer Applications [BPS+17].
  Abstract: Reputation systems are useful to assess the trustworthiness of potential transaction partners, but also a potential threat to privacy since rating profiles reveal users' preferences. Anonymous reputation systems resolve this issue, but make it difficult to assess the trustworthiness of a rating. We introduce a privacy-preserving reputation system that enables anonymous ratings while making sure that only authorized users can issue ratings. In addition, ratings can be endorsed by other users. A user who has received a pre-defined number of endorsements can prove this fact, and be rewarded e.g. by receiving *Premium* member status. The system is based on advanced cryptographic primitives such as Chaum-Pedersen blind signatures, verifiable secret sharing and oblivious transfer.

1.5 Acknowledgements

During the development of this thesis, three research stays have been carried out: a two-week research stay in 2012 at Universidad de Cantabria (Santander, Spain) working with Dr. Daniel Sadornil on bilinear pairings; a three-month research stay in 2014 at Universität des Saarlandes (Saarbrücken, Germany) working with Prof. Dr. Christoph Sorge on the topic of smart metering; and a second two-week research stay in 2015 at Universität des Saarlandes working on the topic of reputation systems.

The first research stay was partially supported by the project *Cryptographic techniques with elliptic and hyperelliptic curves* (Ref: MTM2010-21580-C02-01), funded by MICINN - Ministerio de Ciencia e Innovación. The second and third stays were partially supported by the project *Privacy-preserving and efficient smart metering* (Ref: 57049770), funded by Spanish-German Integrated Actions.

This thesis received a three-year grant for recruitment of early-stage research staff from Generalitat de Catalunya (Ref: 2012FI_B 00917, 2013FI_B1 00122, 2014FI_B2 00036).

This thesis received a grant for its linguistic revision from Institut de Llengües of the Universitat de Lleida (2017 call).

This thesis fulfils the requirements demanded by Universitat de Lleida to obtain the International Doctor Mention.

1.6 Structure of this thesis

This thesis consists of six chapters. The first one is devoted to providing an overview of some concepts related to e-Society. There is a brief classification into the hottest and emerging e-Society branch research topics and the security issues that they have to face. A brief introduction to the object of this thesis, as well as its goals, is given.

In Chapter 2, the cryptographic techniques employed in the design of the proposals presented in this thesis are revised. It starts with a general introduction to public key cryptography. Then, ElGamal cryptosystem along with its additive homomorphic and threshold variations, is described. Subsequently, zero knowledge proofs and secret sharing schemes are presented. Next, an oblivious transfer protocol is explained. Finally, there is a brief introduction to elliptic curve cryptography.

Next, Chapter 3 is devoted to loyalty systems. An overview on related work is given, as well as the main security properties required for such systems. Then, our contribution to this subject is fully detailed.

In Chapter 4 the concept of smart metering is introduced, along with its advantages for both customers and energy suppliers. Then, the privacy concerns arising with smart meter deployment are explained. Related work on this topic is analysed and, finally, our contribution to this topic is presented.

Chapter 5 is focused on reputation systems. Related work is presented, together with a non-exhaustive classification of commercial reputation systems. The main security properties that such platforms should provide are enumerated. Then, our contribution to this subject is fully explained and analysed.

Finally, the last chapter is devoted to highlighting the contributions presented in this thesis, while some possible future work is also enumerated.

– If cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.

Unknown

– If cryptography is outlawed, only outlaws will have privacy.

– Wir müssen wissen, wir werden wissen.[a]

Epitaph on the gravestone of David Hilbert

[a] We must know, we will know.

2 Cryptographic background

This chapter establishes the notation used throughout the thesis. It revises well-known cryptographic techniques employed in the design of the proposals presented in this dissertation. These proposals are intended to deal with the security challenges posed by the e-Society.

First, a general overview to public key cryptography is given. Then, ElGamal cryptosystem is presented, along with its additive homomorphic and threshold variants. Next, Chaum-Pedersen zero knowledge proof is presented, including the basic proof, and the constructions that allow it to be employed for computing signatures and blind signatures. Afterwards, the Shamir secret sharing and Feldman's verifiable secret sharing protocols are detailed. Oblivious transfer protocols are briefly mentioned. Finally, the last section is devoted to elliptic curve cryptography.

2.1 Introduction to public key cryptography

In symmetric key cryptography, a sender and a receiver share a secret key, which is used to encrypt and decrypt messages. Symmetric key cryptosystems are fast and require little computation capacity. Their disadvantage is that the communicating parties need a secure channel to set the secret key. Such a secure channel may be expensive or may simply not exist.

In public key cryptography, each party has a pair of keys, one public and one private. The public one is made available to everybody and is used for encryption and digital signature verification. The private key is kept secret and is used for decryption and for digital signature creation.

The public and the private keys are mathematically linked by a one-way function, so that it is computationally easy to generate the public key from the secret one, but it is computationally infeasible to do it the other way round. Hence, the public key can be published without compromising the secrecy of the private key.

When two parties have to communicate confidentially, the sender asks for the receiver's public key, which is sent through any open channel, not necessarily private. After that, the sender encrypts the message under the receiver's public key and transmits the resulting ciphertext. Finally, the receiver decrypts the ciphertext received using her private key and obtains the cleartext message as a result. The most relevant advantage provided by public key cryptography is that no secure channel is needed for the key exchange.

Public key cryptography was first proposed by Diffie and Hellman in the so-called DH key agreement [DH76]. The security of public key cryptosystems lies in the assumed intractability of some computational hard problems, such as the integer factorization or the discrete logarithm problems. The former is the basis of cryptosystems such as RSA [RSA78] or Paillier [Pai99], while the latter leads to ElGamal cryptosystem [ElG85] and its elliptic curve versions [Kob87, Mil86, HMV03].

Although public key cryptosystems are secure, some attacks may occur during public key exchange. In the classic man-in-the-middle attack, an adversary intercepts parties' public keys and replaces them with fake ones whose secret key is known to it. In this way, an attacked party encrypts the data under a public key whose corresponding private key is known by the attacker. Thus, the attacker is able to decrypt the transmitted ciphertext and access the confidential data while the attacked parties believe they are communicating securely.

In order to avoid this kind of attacks, digital certificates [CIF+03] are used to ensure the authenticity of public keys. A digital certificate is a message relating a public key with the data of its owner. This message is signed by a trusted authority which is assumed to check the validity of the data provided prior to issuing it.

Public key cryptography can be used not only for data encryption, but also for issuing digital signatures. A message is signed by a party by first computing a hash digest of the message and then computing its digital signature by means of an algorithm which takes the message digest and the signer's private key as input. The resulting signature is sent attached to the original message. The receiver validates a digital signature by means of an algorithm that takes as input the message digest computed by herself, the signer's public key and the received digital signature. The result is a boolean indicating whether or not the signature is valid. A valid signature provides *authentication* (the receiver is sure about the identity of the signer), *integrity* (the receiver is sure that the signed message has not been altered during its transmission) and *non-repudiation* (the signer cannot deny having issued a signature).

Sometimes we need a message to be signed by some party who is not autorized to access the message content. In such a situation, we can employ a *blind signature protocol*. Such a protocol is run by two parties, namely the message owner and the signer. As a result, the message owner obtains a signature on her message which validates under the signer's public key while the signer receives no information about the message on which she has computed a signature.

Some public key cryptosystems have an encryption function which offers a homomorphic property [FG07], such that the result of operating two encrypted messages using a given binary operation provides as a result the encryption of the result of operating the two cleartext messages under some other binary operation. Depending on the operation of cleartext messages, the homomorphic cryptosystem can be additive, like Paillier, or multiplicative, like ElGamal or RSA. These cryptosystems may be crucial in systems which need to perform some computations on the encrypted data, so that revealing the original data can be avoided.

Table 2.1 gathers all the cryptographic tools used in the protocols presented in this dissertation, in order to offer a better comprehension.

2.2 ElGamal cryptosystem

ElGamal [ElG85] is a widely known public key cryptosystem whose security is based on the assumed intractability of the discrete logarithm problem (DLP).

Let G be a multiplicative group of order q and let g be a generator of G, $G = \langle g \rangle$. The DLP in group G is stated as follows:

$$\text{Given } g, y \in G, \text{ find an integer } x \text{ such that } g^x = y.$$

Such an integer x is the discrete logarithm of y to the base g ($x = \log_g y$).

There are groups for which solving the DLP is believed to be a hard problem. That is the case, for instance, when G is a large prime order (at least 2048 bit long) subgroup of the group of integers modulo a large prime. Other cryptographically interesting groups include the additive group of points of an elliptic curve or the Jacobian of a hyperelliptic curve defined over a finite field.

The security of several public-key cryptosystems holds on the assumption that the DLP cannot be solved efficiently on such groups.

The fastest known algorithm for solving DLP over $\mathbb{Z}_p^*$ is Index Calculus [SS98], which takes a subexponential time. This algorithm cannot be applied to all groups, for example, over the group of points of an elliptic curve. In this case, Pollard's rho is the best known algorithm, which requires $\mathrm{O}(1)$ memory and $\mathrm{O}(\sqrt{q})$ time, being q the order of the group [MVVO96]. As a result, ElGamal over elliptic curves achieves equivalent security levels using far shorter keys. For example, the security of ElGamal cryptosystem over $\mathbb{Z}_p^*$ taking 2048 bit keys and the security of ElGamal over elliptic curves taking 224 bit keys are equivalent [PP16]. This makes the use of ECC ideal for devices with low computation capacity, such as smart cards or RFIDs.

2.2.1 ElGamal encryption

The ElGamal cryptosystem is composed of four procedures. Set-up and key generation have to be executed once before transmitting secured data. Encryption and decryption are performed every time that a message is sent.

- *Set-up*: Two large primes p and q such that $q \mid p-1$ are chosen. Next, a generator g of the order q multiplicative subgroup G of $\mathbb{Z}_p^*$ is selected. Afterwards, g, p, q are published.

- *Key generation*: A secret key x is generated by taking its value at random $x \in_R \mathbb{Z}_q^*$. The corresponding public key is computed as $y = g^x$.

- *Encryption*: A message $m \in G$ is encrypted under public key y by taking a random $r \in_R \mathbb{Z}_q^*$ and computing $c = g^r$ and $d = m \cdot y^r$. The ElGamal encryption of m under public key y, $E_y(m)$, is the tuple (c, d).

- *Decryption*: A ciphertext $E_y(m)$ is decrypted using the private key x by computing $m = d \cdot c^{-x}$.

Cryptographic technique	Chapter			Use
	Ch 3	Ch 4	Ch 5	
2.2.1 ElGamal encryption		✓	✓	· Smart metering system key generation · Reputation system key generation
2.2.3 Additive homomorphic ElGamal		✓		· Readings with noise encryption and decryption
2.2.4 Threshold ElGamal		✓		· Readings with noise encryption and decryption
2.3.1 Basic CP proof			✓	· Endorsement verification
2.3.2 CP digital signature			✓	· Hotel certificate · Comment signature
2.3.3 CP blind signature			✓	· User certificate obtaining
2.4 Secret sharing			✓	· Secret shares computation and verification
2.5 1-out-of-n oblivious transfer			✓	· Secret share obtaining
2.6.1 Operations in ECC	✓			· Loyalty systems key generation · List $\mathscr{L}$ generation · Coupon masking · Coupon blind signature · Blind signature unmasking
2.6.2 Bilinear pairings	✓			· List $\mathscr{L}$ generation verification i.e. $e(P, Q_{i+1}) = e(Q, Q_i)$ · Coupon signature verification i.e. $e(C_i, Q_k) = e(C_{i+k}, P)$ · Public redeem verification i.e. $e(C_0, Q_n) = e(C_n, P)$
2.6.3 GDH group	✓			· P generates a GDH group

Table 2.1: Summary of the cryptography employed

2.2.2 Multiplicative homomorphic property of ElGamal

ElGamal is a multiplicative homomorphic cryptosystem in the sense that the component-wise product of two ciphertexts provides the encryption of the product of the two cleartext messages.

Let $E_y(m_1) = (c_1, d_1) = (g^{r_1}, m_1 \cdot y^{r_1})$ and $E_y(m_2) = (c_2, d_2) = (g^{r_2}, m_2 \cdot y^{r_2})$ be two ElGamal ciphertexts encrypting m_1 and m_2, respectively. We can obtain an encryption of $m_1 \cdot m_2$ by computing the component-wise product of $E_y(m_1)$ and $E_y(m_2)$. That is,

$$\begin{aligned} E_y(m_1) \cdot E_y(m_2) &= (c_1 \cdot c_2, d_1 \cdot d_2) = \\ &= (g^{r_1+r_2}, m_1 \cdot m_2 \cdot y^{r_1+r_2}) = \\ &= E_y(m_1 \cdot m_2). \end{aligned}$$

2.2.3 Additive homomorphic ElGamal

The ElGamal cryptosystem can be used in such a way that it is additively homomorphic [CGS97] with the integer addition modulo q as group operation. In that case, a message $m \in \mathbb{Z}_q$ is encrypted by performing the ElGamal encryption of $g^m \in \mathbb{Z}_p^*$, that is $E_y(g^m)$. The decryption of $E_y(g^m)$ generates g^m as a result. Hence, an additional discrete logarithm computation is required to obtain m from g^m. This computation can be performed efficiently when m is known to fall in a not too large range by means of Pollard's lambda algorithm [MVVO96].

Note that, given $E_y(g^{m_1})$ and $E_y(g^{m_2})$, then,

$E_y(g^{m_1}) \cdot E_y(g^{m_2}) = E_y(g^{m_1} \cdot g^{m_2}) = E_y(g^{m_1+m_2})$.

2.2.4 Threshold ElGamal

In a public key n-out-of-n threshold cryptosystem, the secret key (required for decryption) is composed of n fragments $x_1, \ldots, x_n$. Each fragment is possessed by a different party. In such a cryptosystem, a ciphertext can only be decrypted if each of the n parties collaborates [DF90, Ped91].

The n-out-of-n threshold ElGamal is an encryption scheme, in which the secret key is distributed among n parties. The public key and the private key fragments are generated by the parties without the need for a trusted dealer.

The *set-up* and *encryption* steps are performed as in the basic ElGamal. Regarding the *key generation* and *decryption* procedures:

- *Key generation*: Each of the n parties, $\mathscr{P}_i$, generates a secret key fragment, by taking a random $x_i \in \mathbb{Z}_q^*$ (this is $\mathscr{P}_i$'s key fragment). Next, each $\mathscr{P}_i$ computes $y_i = g^{x_i}$ and makes y_i public together with a zero-knowledge proof proving knowledge on $\log_g y_i$, for example [Sch90]. The public key is then computed as $y = \prod_{i=1}^{n} y_i$.

- *Decryption*: Given a ciphertext $E_y(m) = (c, d)$, each sharing key party $\mathscr{P}_i$, computes $T_i = c^{x_i}$. This value is called *partial decryption* and has to be made available to those parties allowed to obtain the cleartext. Finally, the cleartext message m is computed as $m = d \cdot (\prod_{i=1}^{n} T_i)^{-1}$.

2.3 Chaum-Pedersen zero knowledge proof

Verifying that some party is in possession of certain information (knowledge) can be as easy as asking her to reveal it. However, in some cases, this knowledge has to be proven without revealing the knowledge itself. In such a situation, a zero-knowledge proof (ZKP) [GMR85] is required.

A ZKP is a protocol by which one party (the prover) can prove to another party (the verifier) that she possesses some knowledge, without giving any information other than the fact that the knowledge is in fact possessed.

2.3.1 Basic proof

Chaum and Pedersen [CP93] presented a method that permits a prover to prove in zero knowledge to a verifier that, given a tuple $(g, g', y, y') \in G^4$, she knows a secret value x satisfying $x = \log_g y = \log_{g'} y'$, where g, g' are generators of G. Given a one-way hash function $\mathscr{H}$, the non-interactive version of this proof is as follows:

1. The prover chooses at random $k \in_R \{1, \ldots, q-1\}$ and computes the tuple $(a, b) = (g^k, g'^k)$.
2. The prover computes $e = \mathscr{H}(a||b)$.
3. The prover computes $r = k + ex \pmod q$ and sends (a, b, r) to the verifier.

The proof is verified as follows:

1. The verifier computes $e = \mathscr{H}(a||b)$.
2. The verifier checks whether $g^r = ay^e$ and $g'^r = by'^e$.

We will denote $CP(g, g', y, y')$ the tuple composed of (g, g', y, y', a, b, r).

Note that this proof may be built over any group with DLP difficulty. Hence, the implementation over elliptic curves is straightforward.

2.3.2 Chaum-Pedersen digital signature

Chaum-Pedersen zero-knowledge proof can be used to compute digital signatures. The signer is required to have an ElGamal private/public key pair.

Given a group generated by g, and with $y = g^x$ being the signer's public key, the tuple $CP(g, \mathscr{H}(m), y, \mathscr{H}(m)^x)$ is a signature on message m [CP93]. $Sign_x(m)$ denotes a signature on message m computed with secret key x.

2.3.3 Chaum-Pedersen blind signature

A blind signature protocol is a form of digital signature involving two parties, Alice and Bob, with the following properties:

- Alice has a message, which should be signed by an authority, Bob.
- Bob cannot learn anything about the content of the message.
- Alice cannot learn anything about Bob's private key.

Given the same parameters as in 2.3.1, a blind signature on the hash of message m, $\mathscr{H}(m)$, can be computed as follows [CP93]:

1. Alice masks the hash $\mathscr{H}(m)$ by computing $m_0 = \mathscr{H}(m)^t$, with $t \in_R \mathbb{Z}_q$, and sends m_0 to Bob.
2. Bob signs m_0 by computing $w_0 = m_0^x$. w_0 is sent to Alice.

Bob proves that $\log_g y = \log_{m_0} w_0$ as follows:

1. Bob computes $(a_0, b_0) = (g^z, m_0^z)$, with $z \in_R \mathbb{Z}_q$ and sends (a_0, b_0) to Alice.
2. Alice computes $a = (a_0 g^{u_2})^{u_1}$, $b = (b_0^{1/t} \mathscr{H}(m)^{u_2})^{u_1}$, with $u_1 \in_R \mathbb{Z}_q^*, u_2 \in_R \mathbb{Z}_q$.
3. Alice computes $w = w_0^{1/t}$ and the challenge $c = \mathscr{H}(\mathscr{H}(m), w, a, b)$.
4. Alice computes the blinded challenge $c_0 = c/u_1 \pmod q$ and sends it to Bob.
5. Bob sends back $r_0 = z + c_0 x$.
6. Alice accepts if $g^{r_0} = a_0 y^{c_0}$ and $m_0^{r_0} = b_0 w_0^{c_0}$.
7. Alice computes $r = (r_0 + u_2)u_1 \pmod q$

The signature on m is given by

$$CP(g, \mathscr{H}(m), y, w_0) = (g, \mathscr{H}(m), y, w, a, b, r).$$

2.4 Secret sharing schemes

Secret sharing schemes are multi-party protocols used to distribute trust or to share control. A secret is divided into pieces (called shares) and distributed amongst n participants (called parties), so that no party is able to recover the original secret without collaborating with some other parties.

Sometimes all shares are required to recover the secret, but there are also threshold schemes, in which any group of t ($t < n$) or more parties can together reconstruct the secret, but any group of fewer than t parties cannot.

2.4.1 Shamir secret sharing

The Shamir secret sharing scheme [Sha79] permits a dealer to share a secret $\sigma \in \{0, \ldots, q-1\}$ among n parties $P_1, \ldots, P_n$ so that σ can only be recovered if at least t shares are known, $t \leq n$. This is called a t-out-of-n-threshold scheme, or (t, n)-threshold, in short. The dealer performs the following procedure:

Given two large primes p, q, such that $q|(p-1)$, let G be the order q multiplicative subgroup of $\mathbb{Z}_p$ and let g be a generator of G, $G = \langle g \rangle$.

1. Choose $t-1$ integers $a_1, a_2, \ldots, a_{t-1} \in_R \{0, \ldots, q-1\}$ at random, $a_{t-1} \neq 0$ and set $a_0 = \sigma$.
2. Consider the polynomial $f(x) = a_{t-1} \cdot x^{t-1} + \ldots + a_1 \cdot x + a_0$ over $\mathbb{Z}_p$.

3. Take n distinct values $X_i \in_R \{1, \ldots, q-1\}$ at random and compute the tuples (X_i, σ_i) with $\sigma_i = f(X_i) \pmod q$.

4. Each party P_i is given a secret share (X_i, σ_i).

In order to recover the secret σ, at least t shares are required. This is because t pairs (X_i, σ_i) with distinct X_i's determine the polynomial $f(x)$ uniquely.

The recovery procedure is straightforward using Lagrange interpolation. Given t shares (X_i, σ_i) the secret is obtained by computing $\sigma = f(0) \pmod q$.

Secret σ can be obtained directly by computing,

$$\sigma = \sum_{i=0}^{t} \sigma_i \cdot \lambda_i \pmod q, \tag{2.1}$$

with $\lambda_i = \prod_{\substack{j=0 \\ i \neq j}}^{t} \frac{X_j}{(X_j - X_i)} \pmod q$.

2.4.2 Verifiable secret sharing

Shamir secret sharing scheme presents the following drawbacks:

- A corrupted dealer could provide badly generated shares.
- A dishonest party could disrupt the secret recovery process by providing a wrong share.

Feldman [Fel87] proposed a verifiable secret sharing scheme based on Shamir's scheme. The secret $\sigma \in \{0, \ldots, q-1\}$ is shared among n parties $P_1, P_2 \ldots, P_n$. Let g be a generator of G. Then, the dealer proceeds as follows:

1. Choose $t-1$ integers $a_1, a_2, \ldots, a_{t-1} \in_R \{0, \ldots, q-1\}$ at random, $a_{t-1} \neq 0$.

2. Build the polynomial $f(x) = a_{t-1} \cdot x^{t-1} + \ldots + a_1 \cdot x + a_0$, such that $a_0 = \sigma$.

3. Compute n shares (X_i, σ_i), with $X_i \in_R \{1, \ldots, q-1\}$, and $\sigma_i = f(X_i) \pmod q$.

4. Compute $c_j = g^{a_j}$, for $j = 0, 1, \ldots, t-1$. Note that $c_0 = g^{a_0} = g^{\sigma}$.

5. Commit to polynomial f by broadcasting $c_0, c_1, \ldots, c_{t-1}$. Next, she sends each share (X_i, σ_i) to P_i, $\forall i = \{1, \ldots, n\}$.

Whenever a party receives a share (X_i, σ_i), she can check whether it fulfils:

$$g^{\sigma_i} = \prod_{j=0}^{t-1} (c_j)^{{X_i}^j}, \tag{2.2}$$

taking all the arithmetic modulo p. Note that this equality holds since:

$$g^{f(X_i)} = \prod_{j=0}^{t-1} (g^{a_j})^{{X_i}^j} = g^{a_0} \cdot g^{a_1 \cdot X_i} \cdot g^{a_2 \cdot {X_i}^2} \cdots g^{a_{t-1} \cdot {X_i}^{t-1}}.$$

In order to recover the secret σ, at least t participants $P_1, P_2, \ldots, P_t$ must cooperate. Each P_i provides her share (X_i, σ_i). Upon reception of (X_i, σ_i), its validity can be verified by checking whether 2.2 holds. If all shares are valid, the secret σ can be computed as in 2.1.

2.5 1-out-of-n oblivious transfer

A 1-out-of-n oblivious transfer protocol involves two parties: a sender who is in possession of n pieces of information and a receiver. As a result of a protocol execution, the receiver obtains one of the pieces without the sender receiving any knowledge about which element was actually queried, while the receiver does not learn any information about the elements that were not retrieved. In a k-out-of-n oblivious transfer protocol the receiver obtains k pieces of information.

The proposal [OK04] provides an efficient adaptive k-out-of-n oblivious transfer proposal which can serve our purposes by setting $k = 1$. Its communication cost is $O(n)$. They introduce the notion Oblivious Keyword Search (OKS). In such a protocol, the pieces of information are in a database and the receiver can search and retrieve data that contain some chosen keywords. The sender does not learn anything from the chosen words.

Commit phase:

- The sender generates an RSA private/public key pair [RSA78]. The private key d is kept secret while the public key (N, e) is made public.
- The sender takes each of its n keywords M_i, $i = 1, \ldots, n$, and computes, $K_i = \mathscr{H}(i)^d \pmod n$, and $E_i = G(K_i||i) \oplus M_i$. G denotes a pseudo-random bit string generator.
- The sender sends $E_1, \ldots, E_n$ to the receiver.

Transfer phase:

- The receiver takes an index i_j and asks the sender to blindly sign it under the RSA blind signature protocol [Cha83].
- As a result, the receiver obtains $K_{i_j} = \mathscr{H}(i_j)^d \pmod n$ which is the key for decrypting E_{i_j} generating the keyword M_{i_j} as output.

2.6 Elliptic curve cryptography

This section provides some background on elliptic curves, bilinear maps and Gap Diffie-Hellman groups, focused on their applications to cryptography.

2.6.1 Elliptic curves

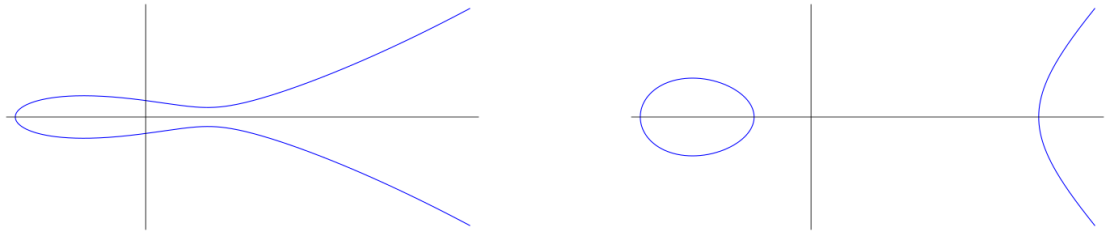
An elliptic curve E defined over a finite field $\mathbb{F}_{p^k}$ is an algebraic curve without singular points and is given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2{}_1x + a_6, a_i \in \mathbb{F}_{p^k},$$

denoted as Weierstraß general equation.
If the characteristic is $p \neq 2, 3$, and using linear transformations, the curve can be expressed as

$$y^2 = x^3 + ax + b, \tag{2.3}$$

denoted as reduced Weierstraß equation. The polynomial discriminant must be different from 0, *i.e.* $4a^3 + 27b^2 \neq 0$, so that the curve has no singularities (see [Sil09]).

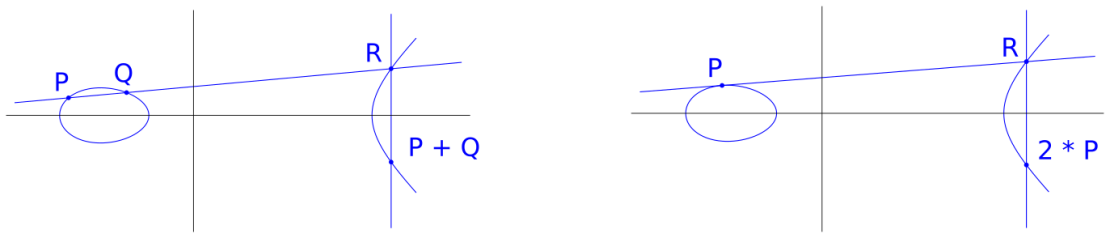


(a) $y^2 = x^3 - 3x + 3$ **(b)** $y^2 = x^3 - 13x - 12$

Figure 2.1: Elliptic curves over $\mathbb{R}$

If $E/\mathbb{F}_{p^k}$ is a curve over $\mathbb{F}_{p^k}$, then we denote by $E(\mathbb{F}_{p^k})$ the set of points $P = (x, y) \in \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ that satisfy the curve equation, along with the point at infinity $\mathcal{O}$.

An addition operation can be defined over $E(\mathbb{F}_{p^k})$ using the chord-tangent method. This method takes the line r that goes through P and Q and computes the third point R over the curve (if $P = Q$, then R is the tangent point to the curve). The point $P + Q$ (or $2 \cdot P = P + P$) is the intersection between the curve and the line that goes through R and $\mathcal{O}$.



(a) $y^2 = x^3 - 3x + 3$ **(b)** $y^2 = x^3 - 13x - 12$

Figure 2.2: Elliptic curve point addition and doubling in $\mathbb{R}$

This operation endows the set $E(\mathbb{F}_{p^k})$ with an abelian group structure in which $\mathcal{O}$ is the identity element.

Analytically, given a equation of the form 2.3, if $P = (x_1, x_2), Q = (x_2, y_3)$ and if $P + Q \neq \mathcal{O}$, then the coordinates of point $P + Q = (x_3, y_3)$ are given by

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = (x_1 - x_3) \cdot \lambda - y_1, \end{cases}$$

where $\lambda = \dfrac{(y_1 - y_2)}{(x_1 - x_2)}$ if $x_1 \neq x_2$ and where $\lambda = \dfrac{(3 \cdot x_1^2 + a}{(2 \cdot y_1)}$ if $x_1 = x_2$ and $y_1 \neq 0$. The opposite point of $P = (x, y)$, $-P$, has coordinates $(x, -y)$.

The computational cost of adding two points requires one inversion and three multiplications over the base field, while the doubling requires one inversion and four multiplications.

Considering the group law, a point $P \in E(\mathbb{F}_{p^k})$ can be multiplied by a scalar x as follows

$$xP = \underbrace{P + \cdots + P}_{x \text{ times}}.$$

The point xP can be computed in an efficient way using the double-and-add algorithm.

The *elliptic curve discrete logarithm problem* (ECDLP) consists, given two points P and Q such that $Q = xP$, of finding an integer x that solves the equation. This is a computationally hard problem. Elliptic curve cryptography (ECC) has been extensively used since its introduction in 1985, due to the fact that the size of the keys, storage and transmission requirements are significantly smaller than in other cryptosystems, such as RSA [HMV04].

These features make ECC suitable for electronic devices with small computational power, such as RFIDs or smart cards.

2.6.2 Bilinear maps

Let G_1, G_2 and G_t be cyclic groups of the same order. A *pairing* is a bilinear map

$$e : G_1 \times G_2 \longrightarrow G_t,$$

satisfying the *bilinearity* property:

$$e(aP, bQ) = e(P, Q)^{ab}, \quad \forall P \in G_1,\ Q \in G_2, \text{ and } a, b \in \mathbb{Z}.$$

with two additional properties:

- *Non-degeneracy*: For each $P \in G_1$, there exists $Q \in G_2$ such that $e(P, Q) \neq 1$.
- *Computability*: There exists an efficient algorithm to compute $e(P, Q)$ for any pair $P \in G_1$, $Q \in G_2$.

Pairings were first used in cryptanalysis to attack discrete logarithm-based systems on a certain class of elliptic curves [MOV91]. However, it was shown that they could also be successfully used as building blocks for the design of new cryptographic protocols, such as identity-based encryption schemes [BF01] or short signatures [BLS04] (see Barreto's compendium on pairing-based cryptography [Bar09]).

In this thesis, the pairing considered is $e : G \times G \longrightarrow G_t$, where G, G_t are subgroups of the group of points of an elliptic curve E.

Given an elliptic curve (E) over $\mathbb{F}_{p^k}$, with characteristic $char(\mathbb{F}_{p^k}) > 3$, a divisor (D) is defined as:

$$D = \sum_{P \in E} i_P[P],$$

where i_P is an integer, P is a point of $E(\mathbb{F}_{p^k})$ and $[P]$ is a formal symbol.

A principal divisor of a rational function is defined as follows:

$$div(f) = \sum_{P \in E} ord_P(f)[P],$$

where f is a rational function over E.

The most well-known is Weil pairing (e_n) and its definition is as follows:

$$e_n(P, Q) = \frac{f_Q(D_P)}{f_P(D_Q)},$$

where $P, Q \in E(\mathbb{F}_{p^k})[n]$, $D_P = [P] - [\mathcal{O}]$, $D_Q = [Q] - [\mathcal{O}]$, f_P, f_Q are pairing evaluation functions such that $div(f_P) = n[P] - n[\mathcal{O}]$, $div(f_Q) = n[Q] - n[\mathcal{O}]$ and a function evaluated at a divisor is computed as:

$$f\left(\sum_{P \in E} i_P[P]\right) \stackrel{def}{=} \prod_{P \in E} f(P)^{i_P}, \quad f\left(\sum_{Q \in E} i_Q[Q]\right) \stackrel{def}{=} \prod_{Q \in E} f(Q)^{i_Q}$$

2.6.3 Gap Diffie-Hellman groups

Let G be the multiplicative cyclic group generated by an elliptic curve point P of prime order q. We consider the following two problems on G:

- *Decision Diffie-Hellman (DDH) problem*: Given a tuple (P, aP, bP, cP) decide whether $c = ab$, for $a, b, c \in \mathbb{Z}_q^*$.
- *Computational Diffie-Hellman (CDH) problem*: Given (P, aP, bP) compute abP, for $a, b \in \mathbb{Z}_q^*$.

A Gap Diffie-Hellman (GDH) group, is a group in which the DDH problem can be decided efficiently while the CDH problem is presumably hard [Bol03]. The DDH problem is usually decided employing a bilinear operation defined on G. In such a case, we can check whether (P, aP, bP, cP) is a DDH tuple by verifying whether $e(P, cP) = e(aP, bP)$.

GDH groups are appropriate to implement discrete logarithm-based cryptography [Bol03]. Let $G = \langle P \rangle$ be a GDH group of prime order q. A user creates her private key by choosing an integer $x \in_R \mathbb{Z}_q^*$ at random. Next, the public key is generated as $Q = xP$.

Let M be a message and let $\mathscr{H}$ be a cryptographic hash function generating an element of G as output. In a GDH group, M can be digitally signed by computing $S = x\mathscr{H}(M)$. A signature S on M is verified by checking that $(P, \mathscr{H}(M), Q, S)$ is a valid DDH tuple.

– "But it does not seem that I can trust anyone", said Frodo. Sam looked at him unhappily. "It all depends on what you want", put in Merry. "You can trust us to stick with you through thick and thin–to the bitter end. And you can trust us to keep any secret of yours–closer than you keep it yourself. But you cannot trust us to let you face trouble alone, and go off without a word. We are your friends, Frodo."

J.R.R. Tolkien, The Fellowship of the Ring

3 Loyalty systems

This chapter is devoted to loyalty systems. An overview on related work is given including the basic security properties to be provided. After that, we focus our analysis on a proposal by Enzmann et. al [EFS04] which is shown to include two limitations. Our contribution to this subject, published in Proceedings of XIV Reunión Española sobre Criptología y Seguridad de la Información [BSV16], is an enhancement to the aforementioned paper which solves the mentioned limitations.

Loyalty systems are structured marketing strategies whose goal is to reward, and hence strengthen, loyal behaviour of customers.

The beginnings of customer loyalty systems were in the late 18th century [McE14], when American retailers gave copper tokens with purchases that could be redeemed in future transactions.

The first third-party loyalty programme was introduced in the USA in 1896 by Sperry & Hutchinson (S&H). Customers in supermarkets or petrol stations gained Green Stamps according to how much they spent purchasing. The Green Stamps were pasted into booklets, which could be redeemed (when completed) to obtain a reward, such as household products or personal items.

Nowadays, they have a website (www.greenpoints.com) where to trade in old Green Stamps for greenpoints and redeem them for gift cards or certificates.

Over the last century the amount of loyalty systems has increased tremendously. The importance of loyalty programmes in the real economy is reflected in the amount of loyalty programmes nowadays: according to [Ber13], in 2012 there were 2.65 billion memberships in the USA. This huge impact is encouraging companies to redefine their programmes to benefit from the customers' extensive use of modern technologies, such as Internet communications, mobile devices, smart cards or RFID tokens.

Most successful loyalty programmes are based on one (or more) of the following ideas:

- *Loyalty-points system*: this is the most common technique. Every time a customer performs a purchase, she receives some loyalty-points depending on the amount

Figure 3.1: Green Stamps, Sperry & Hutchinson, 1896

invested. When enough of them have been collected, she can redeem them to obtain a reward, which can be a discount or a freebie. An example is given by the frequent-flyer-programmes offered by many airlines. These loyalty-points are often presented as coupons, a piece of (paper-based or electronic) information which is worth some loyalty-points.

- *Rewards for initial loyalty*: in this case, the reward is granted at the beginning, trying to hook potential customers. This could be the case of Google Play Music or Netflix, offering some-months free trial.

- *Privileges for VIPs*: the customers pay a fee to obtain some advantage over the other customers, who pay less or even nothing. This is the case of Amazon Prime. If a customer decides to pay the Amazon Prime fee, she will receive all the products marked as "Prime" (which are a lot) with free shipping costs; while a normal customer has to pay for shipping every time she buys something. Currently it also gives access to Amazon Video. They also offer a 30-day free trial (a reward for initial loyalty).

- *Partnership*: two or more companies have an agreement to make better offers, for those customers who use both services. This is the case of Dropbox and Samsung. If a customer links her Samsung product to her Dropbox account, she receives 48 GB of space, for up to two years, at the same time boosting the need to buy a new mobile every two years.

- *Non-monetary programmes*: the reward is neither money nor discounts. In this case, the customer shares an interest with the company, such us being eco-friendly or raising money for a cause the customer cares about. For example, Dell has been recovering used electronics (104.7 million kg) and using them as post-consumer recycled plastics. It offers green packaging and has also reduced the energy intensity and the operational emissions. They also have a member purchase programme and discounts for students.

- *Unique product*: when the customer is captivated by a product, the loyalty is long-lasting. This is the case of Apple. They offer neither the best prices nor the best quality, but their customers are simply "charmed".

Among loyalty strategies, coupon systems have been widely used. With these systems, companies try to influence customers' buying behaviour by providing them with a *coupon* [CGH06, Esc07, YK11] after each purchase. A coupon is a piece of (paper-based or electronic) information which is worth some *loyalty-points*, depending on the amount of money spent. When enough loyalty-points have been collected, they can be redeemed for some benefit such as a discount for a future purchase or a present.

A coupon system can be *token-based* [ES05] or *counter-based* [EFS04, ES05]. With a token-based system, the user receives one or several tokens after each purchase. All these tokens have to be stored by the customer until they are redeemed (as in e-coin systems). On the contrary, with a counter-based system, the customer keeps just one counter that is increased with each purchase. The advantages of counter-based systems derive from the fact that the required storage capacity is kept constant, so that it requires less bandwidth and less computation time for the vendor's verification protocol.

Vendors take advantage of coupon systems in two ways. On the one hand, they increase the number of casual customers and try to turn them into loyal ones. On the other hand, by asking customers to identify themselves, they can create a customer database and exploit the information collected for many purposes such as price discrimination or direct marketing. The information stored in such databases is very sensitive since it contains personal information as well as the user's buying behaviour.

In contrast to paper-based coupons, it is really easy to produce an identical copy of an electronic coupon. Further, a malicious customer could try to manipulate her coupons. For this reason, electronic coupon systems should satisfy the following security properties:

- *Unforgeability*: Only the vendor can issue valid coupons. It must not be possible for any other to generate a new coupon or increase the number of loyalty-points (in counter-based systems).
- *Double-spending detection*: Each coupon can only be redeemed once. The vendor must be able to notice if a given coupon has already been redeemed.
- *Privacy*: Nobody can trace the amount of loyalty-points of a given customer. Moreover, different coupon operations cannot be linked.
- *Verifiability*: All protocol operations must be verifiable so as to check their correctness. Public verifiability is attained when verifications can be performed using public information.

3.1 Related work

For the sake of preserving customer privacy, Wibowo et al. [WLT00] proposed the idea of using blindly signed pseudo-digital certificates. That solution preserves customer privacy while satisfying the requirements of a loyalty programme scheme.

A multi-coupon [CES+05] refers to a collection of coupons that is handled as a single unit in such a way that *unsplittability* is provided, that is, two users cannot redeem coupons from the same multi-coupon separately and independently at the same time. Chen et al. [CES+05] proposed a secure multi-coupon system that permits customers to redeem a predefined number of coupons from the same multi-coupon. Later, Nguyen [Ngu06] introduced an unforgeable privacy-protecting multi-coupon system, with constant communication and computation complexity. Both proposals were improved in [CEL+07] by

introducing that single coupons from the same multi-coupon can represent different goods or services.

Enzmann et al. proposed two counter-based loyalty systems. The first one [EFS04] uses discrete logarithm-based cryptography while the second one [ES05] is constructed over the RSA cryptosystem. The user generates a random number which is blindly signed by the vendor each time the user obtains a loyalty-point. An n-times multi-signed number represents an n-loyalty-points coupon.

Lately, loyalty systems that can be applied in a multi-vendor scheme have been proposed [AEL+08, IDHFGPC11], as well as some solutions to manage vouchers and mobile coupons using NFC [BJGG+13, OIV+14]. A survey of proposals in the customer loyalty field is given in [TRP13].

In Section 3.3, an enhancement of [EFS04] (hereinafter, referred to as EFS) is presented, extending it with two additional features:

- The counter can be incremented by several units in just one step, instead of executing the issue protocol repeatedly for each point issued.

- All the operations are publicly verifiable; thus, anyone can check whether the protocols are run faithfully.

Our proposal offers improved performance, which is especially relevant when implemented on resource constrained devices. Furthermore, short-time transactions are worthwhile, since they provide a better user experience.

3.2 The EFS coupon system

The EFS coupon system is established by a single vendor, whose goal is to gain loyal customers. Every customer can join the system by acting independently. After each purchase, a given customer and the vendor interact, so that the customer gains proof of her loyalty. For such a purpose, the vendor provides the customer with one loyalty-point, which is reflected in a coupon. The coupon is represented by a tuple (ς, i, C_i), where ς can be seen as a serial number, i is the number of loyalty-points at a given moment and C_i is a cryptographic object that provides security in the sense that the coupon cannot be manipulated. After gaining n loyalty-points, the customer can claim some reward.

More in detail, this system is performed in the following four stages:

- *Set-up:* The vendor sets some cryptographic parameters and its private/public key pair. This stage is performed once at the beginning, when setting up the system.

- *Coupon initialization:* When joining the system, the customer creates a new coupon with zero loyalty-points.

- *Issue:* After each purchase, the customer and the vendor interact. As a result, the number of loyalty-points of the customer is increased by one unit.

- *Redeem:* Once the customer has gained n loyalty-points, she redeems them. The vendor checks the correctness of the procedure and, if so, stores ς in the database and provides the customer with the reward.

Set-up The vendor chooses an appropriate elliptic curve E and a point P such that the subgroup generated by P is a GDH group, the order of this group is a large prime p and $p-1$ does not have small factors.

The vendor chooses a random secret value $x \in_R \mathbb{Z}_p^*$ and computes her public key $Q = xP$. Next, she publishes the pair (P, Q), the curve E, a cryptographic hash function $\mathscr{H}$ (mapping elements from $\mathbb{Z}$ to $G = \langle P \rangle$) and a special finite set $\mathbb{S} \subset \mathbb{Z}$ which is defined by the vendor. Some examples showing how to create this set can be found in [Cha89].

Coupon initialization The customer chooses a random number $\varsigma \in_R \mathbb{S}$, computes $C_0 = \mathscr{H}(\varsigma)$ and stores $(\varsigma, 0, C_0)$.

Issue Supposing that the customer counter is (ς, i, C_i), with $C_i = x^i C_0$, it will be incremented to $(\varsigma, i+1, C_{i+1})$, with $C_{i+1} = x^{i+1} C_0$, so that an additional loyalty-point is added. The following steps are conducted:

1. The customer randomly chooses $r_i \in_R \mathbb{Z}_p$, blinds her current counter by computing $B_i = C_i + r_i P$ and sends B_i to the vendor.
2. The vendor signs B_i by computing $D_i = xB_i$ and sends D_i to the user.
3. Afterwards, the customer unblinds D_i by computing $C_{i+1} = D_i - r_i Q$ obtaining $C_{i+1} = xC_i$. Next, she verifies whether the vendor has sent a correct response by verifying that (C_i, P, C_{i+1}, Q) is a valid DDH tuple, which can be done by checking $e(C_i, Q) = e(C_{i+1}, P)$. If the verification succeeds, the customer stores $(\varsigma, i+1, C_{i+1})$.

Redeem When the user reaches some redeeming threshold n, she sends the tuple (ς, n, C_n) to the vendor, who can check the validity of the loyalty-points by checking whether $C_n = x^n \mathscr{H}(\varsigma)$. If the previous verification succeeds and ς is not in the database of already redeemed serial numbers, she stores it there and sends the reward to the customer.

The EFS system presents, though, two limitations:

- The loyalty-points counter is increased one-by-one. If some purchase is granted with k loyalty-points, the issue operation has to be executed k times.
- The checking performed in the *redeem* operation requires knowledge of the secret key x. Therefore, it can only be carried out by the vendor. In case of dispute, it could only be resolved by revealing the private key x; hence, it is not publicly verifiable.

3.3 Publicly verifiable counter-based proposal

The proposal presented in Figure 3.2 is an extension of the EFS system, providing two additional features:

- The counter can be increased by several loyalty-points in a single operation.
- It provides public verifiability.

The protocol proceeds following the stages below:

Set-up The coupon initialization is performed as in Section 3.2 but some additional information is published by the vendor:

- A list $\mathscr{L} = \{Q_0, Q_1, \ldots, Q_m\}$, where $Q_0 = P$, $Q_{i+1} = xQ_i$, for $i = 0, \ldots, m-1$, and m is the amount of loyalty-points required to obtain the most valuable reward.
- The generation of list $\mathscr{L}$ is proven to be correct by means of bilinear pairings[1] by checking: $e(P, Q_{i+1}) = e(Q, Q_i)$.

Coupon initialization As in Section 3.2, the customer chooses a random $\varsigma \in_R \mathbb{S}$, computes $C_0 = \mathscr{H}(\varsigma)$, checks that $C_0 \neq P$ and stores $(\varsigma, 0, C_0)$. If $C_0 = P$, a different ς is taken.

The set $\mathbb{S}$ must be defined so that the probability that two different customers take the same value ς is negligible. This is achieved if $\mathbb{S}$ has a large cardinality (at least 256 bit long).

Issue Let us assume that a customer's current coupon is (ς, i, C_i) and she has performed some purchase so that she will receive k additional loyalty-points.

1. The customer randomly chooses $r_i \in_R \mathbb{Z}_p$, blinds her current counter value by computing $B_i = C_i + r_i P$ and sends B_i to the vendor.
2. Next, the vendor blindly signs B_i by computing $D_i = x^k B_i$ and returns D_i to the customer.
3. Finally, the customer unblinds D_i by computing $C_{i+k} = D_i - r_i Q_k$. Next, she verifies that the vendor has sent a correct value by verifying whether (C_i, C_{i+k}, P, Q_k) is a valid DDH tuple, in which case $C_{i+k} = x^k C_i$. This verification can be done by checking $e(C_i, Q_k) = e(C_{i+k}, P)$. If the verification succeeds, the customer updates her coupon to $(\varsigma, i+k, C_{i+k})$.

Redeem When the user reaches some redeeming threshold n, $n \leq m$, she sends the tuple (ς, n, C_n) to the vendor who can check the validity of the loyalty-points by checking $C_n = x^n C_0$. If it is correct, $C_0 \neq P$ and ς is not in the database of redeemed serial numbers, then the vendor contacts a Time Stamp Authority (TSA) in order to obtain a trusted timestamp [ANS12] for ς. Next, the vendor stores both ς and its timestamp in the database and sends the reward to the customer. Otherwise, no compensation is given. Note that the validity of (ς, n, C_n) can be publicly checked by anyone by verifying that (C_0, C_n, P, Q_n) is a valid DDH tuple.

If a malicious customer tried to redeem the same coupon more than once, the vendor would detect this situation after finding ς in the database. The vendor could prove that the received coupon had been redeemed before by showing the timestamp for ς generated just after the first redemption.

A malicious vendor could claim that the value ς received from an honest customer has already been redeemed. In such a situation, the vendor would not be able to provide a proper timestamp for ς so that vendor's claim would not be credible.

[1] Note that this could also be checked using Chaum-Pedersen's proof (see Section 2.3.1). The vendor publishes a zero-knowledge proof showing that $\log_{Q_i} Q_{i+1} = \log_P Q$, for $i = 0, \ldots, m-1$. Indeed, this is the way it was proposed in [BSV16].

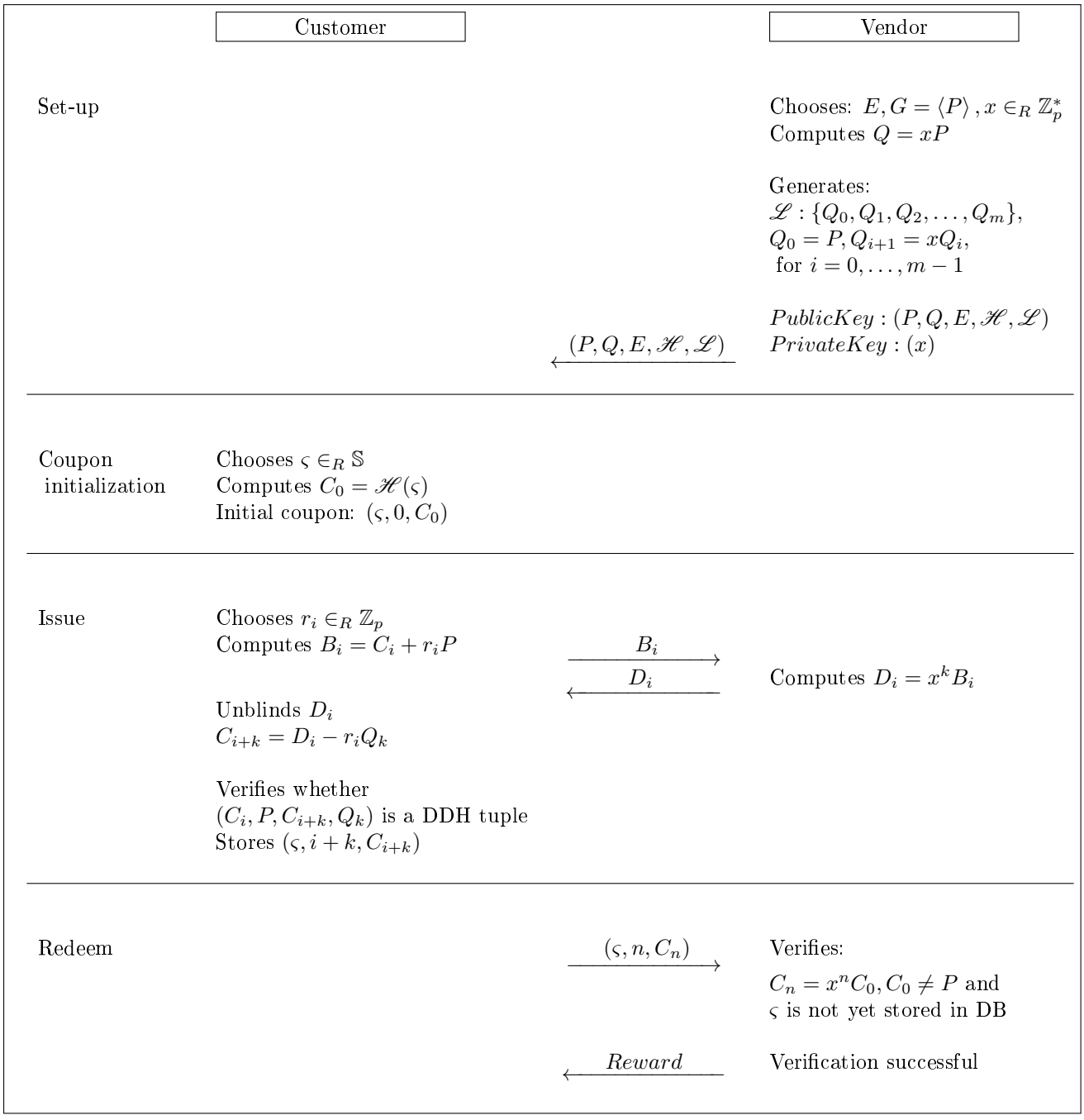


Figure 3.2: Publicly verifiable counter-based loyalty system

Note that, with this scheme, if a customer's purchase is granted with k loyalty-points, the counter can be increased by k units in constant $O(1)$ time.

Furthermore, due to the incorporation of the public list $\mathcal{L}$ to the protocol, the verification performed in the redeem phase can be carried out using only publicly available information; thus, anyone can verify it.

Performance Table 3.1 shows a performance comparison, in terms of communication (measured in bits) and computation, between the EFS system and ours, where:

- $size_{ECPoint}$: denotes the amount of bits required to represent an elliptic curve point.
- $cost_{mult}$: denotes the cost of a scalar product between an integer and an elliptic curve point.
- $cost_{pair}$: denotes the cost of a pairing computation.

This analysis has assumed as negligible the cost of adding two elliptic curve points when compared to the cost of a scalar product or a pairing computation.

Table 3.1: Performance comparison

	EFS	Ours
Communication	$k \cdot (2 \cdot size_{ECPoint})$	$2 \cdot size_{ECPoint}$
Computation	$k \cdot (cost_{mult} + cost_{pair})$	$cost_{mult} + cost_{pair}$

It can be seen that our system has a constant cost that equals the performance of the EFS system when $k = 1$ and is more efficient when $k \geq 2$. The gain is k.

3.4 Security analysis

The security requirements stated at the beginning of this chapter are fulfilled by the scheme presented above: unforgeability, double-spending detection, privacy and public verifiability.

Unforgeability The proposal presented in the previous section is an enhancement of the EFS system [EFS04]. There, it is proven that, under the assumption that the *incremental Diffie-Hellman problem* is hard, a coalition of malicious customers cannot redeem more loyalty points than those issued by the vendor. This problem will be referred to as the EFS problem. Next, this problem is described in a formal manner.

The EFS problem: Let E be an elliptic curve and let the point P be a prime order GDH group generator. Let $Q = xP$ (the integer x is not known) and let $\{\mathscr{C}_1, \ldots, \mathscr{C}_k\}$ be a set of chains so that each chain $\mathscr{C}_i$ is of the form $\{C_0^{(i)}, xC_0^{(i)}, x^2C_0^{(i)}, \ldots, x^{n_i}C_0^{(i)}\}$ for some n_i satisfying $1 \leq n_i \leq m$ (m is the maximum length a chain can have). All the elements in these chains belong to the GDH group chosen during the set-up.

Given these input values, the EFS problem consists of finding either:

(i) An elliptic curve point $x^{t_i}C_0^{(i)}$ with $t_i > n_i$, for some $i \in \{1, \ldots, k\}$.

(ii) A pair of elliptic curve points C_0 and x^tC_0 with $0 < t \leq m$, satisfying that $C_0 \neq C_0^{(i)}$ for each $i \in \{1, \ldots, k\}$, and an integer $\varsigma \in \mathbb{S}$ such that $C_0 = \mathscr{H}(\varsigma)$.

In the former case, the coalition would be able to increase the loyalty points counter of a coupon. In the latter case, the coalition would be able to forge a new coupon containing t loyalty points.

We will denote EFS$(E, P, xP, m, \{\mathscr{C}_1, \ldots, \mathscr{C}_k\})$ an algorithm that solves the aforementioned problem in polynomial time. As already mentioned, in [EFS04] it was proven that such an algorithm cannot exist.

Forgery in our enhanced proposal can be stated in a similar manner to in EFS. The only difference is that, in our proposal, not only a public key point $Q = xP$, but also a list $\mathscr{L} = \{Q_0, Q_1, \ldots, Q_m\}$ with $Q_i = x^i P$ is provided. We will denote eEFS$(E, \mathscr{L}, m, \{\mathscr{C}_1, \ldots, \mathscr{C}_k\})$ an algorithm that solves the aforementioned (enhanced) problem in polynomial time.

Next, it will be proven that an efficient algorithm to solve the *eEFS* problem cannot exist since it could be used for efficiently solving the *EFS* problem.

Theorem. *If the EFS problem is hard, then the eEFS problem is also hard.*

Proof. Let us assume that there exists an algorithm that solves the eEFS problem efficiently. Below, it will be shown how it could be employed to solve the EFS problem.

Let $E, P, xP, m, \{\mathscr{C}_1, \ldots, \mathscr{C}_k\}$ be an instance of the EFS problem. An algorithm EFS$(E, P, xP, m, \{\mathscr{C}_1, \ldots, \mathscr{C}_k\})$ would proceed as follows.

Let i be an index so that the length of $\mathscr{C}_i$ is larger or equal to all other chain lengths (this length is $n_i + 1$). Without loss of generality, it will be assumed that $i = 1$ (the chains $\mathscr{C}_1, \ldots, \mathscr{C}_k$ can easily be renamed to satisfy this assumption).

Make a call to eEFS$(E, \mathscr{C}_1, n_1, \{\mathscr{C}_2, \ldots, \mathscr{C}_k\})$, take its output and return it as the output of EFS$(E, P, xP, m, \{\mathscr{C}_1, \ldots, \mathscr{C}_k\})$. This procedure would return a valid solution to the EFS problem in polynomial time. Hence, a polynomial time algorithm for the eEFS problem cannot exist.

Double-spending detection This property prevents customers from redeeming a coupon more than once. It is fulfilled because whenever the vendor accepts to redeem a coupon, its serial number ς is stored so that it will not be accepted again.

Privacy As in [EFS04], privacy is provided since the vendor only has access to a blinded version of the current counter C_i. The blinded value B_i is uniformly and independently distributed and cannot be linked to C_i. Such a construction also provides *unlinkability* in the sense that different executions of the issue protocol cannot be related.

Public verifiability When the customer wants to redeem n loyalty-points, she hands over her coupon (ς, n, C_n). The validity of that coupon can be publicly verified by anyone just by checking whether $(\mathscr{H}(\varsigma), P, C_n, Q_n)$ is a valid DDH tuple. This operation involves only public data.

– I think privacy is valuable. You don't have to share everything, and it's healthy to occasionally hit the pause button and ask yourself if you're oversharing. But at the end of the day, if you're not doing anything wrong, you don't have anything to hide.

Ashton Kutcher

– Ich habe keine besondere Begabung, sondern bin nur leidenschaftlich neugierig.[a]

Albert Einstein

[a] I have no special talent, I am only passionately curious.

4

Smart metering systems

This chapter introduces the concept of smart metering technologies, presenting their advantages for customers and energy suppliers, together with the privacy concerns arising from their massive deployment. Related work on this topic is analysed including a taxonomy, composed of three main paradigms, for privacy-preserving smart metering solutions. Finally, our contribution, published in the Computer Communications journal [BPS+16], is fully detailed.

Smart meters are a refined adaptation of traditional electricity meters. These devices record energy consumption in small intervals of time, for example every 30 minutes, and regularly communicate their readings to the utility for monitoring and billing purposes. They can provide quick, accurate measurements of electricity use without the need for estimated monthly bills or visits from meter readers.

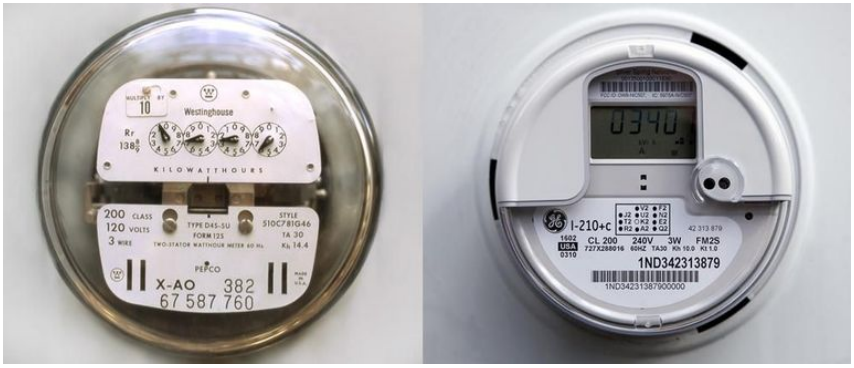


Figure 4.1: Analogic meter vs smart meter

Smart meters have been set up in many countries around the world since the early 2000s [AY16a]. USA and Europe have been deploying smart meters for many years, while other regions of the world such as Australia and Canada have just started. By the end of 2016, there were an estimated 700 million smart meters installed worldwide, half of them

in China [Ele17]. The EU aims to replace at least 80% of electricity meters with smart meters by 2020 wherever it is cost-effective [Eur17].

An efficient and effective treatment of energy has become an important conceptual paradigm for future social and economic energy use, since non-renewable energy resources are limited. Moreover, electricity cannot be stored in large quantities; for this reason, it is highly useful for energy suppliers to keep track of the current energy consumption, as well as knowing its trend. In this way, they can adapt their trades at the energy exchange, and—in the long run—avoid the production of an electricity surplus. Smart metering is an appropriate technology for monitoring, measuring and making predictions of energy utilization, which results in advantages for both energy suppliers and final customers.

The benefits for consumers are the following:

- Consumers can be informed about energy cost, energy consumption and related carbon emission data in real time. The historical data of this information is available online.
- Energy consumption of household gas, electrical and water equipment is displayed on the smart meter.
- Multi-tariff functions are available. This permits consumers to reduce costs by increasing energy consumption during off-peak periods.

The utilities can track real energy consumption and compare it to current production, so that they can:

- Prepare an energy plan to avoid unnecessary energy production.
- Try to promote electricity consumption at times of higher availability by influencing the energy consumption of their users.

These are not the only advantages, since the companies will benefit from support in demand response techniques, a reduction in 'costs to serve', a new communication channel with customers, and so on.

There also exist benefits for the environment, since the emission of CO_2 has been proven to be reduced after the deployment of smart meters [MNDA+17].

However, smart meters have raised concerns about being privacy invasive. Meter readings allow behavioural patterns to be inferred, such as the time at which a given customer leaves her home, switches on the washing machine or goes to bed. For this reason, smart metering solutions should provide mechanisms for customer privacy preservation.

4.1 Related work

Research on smart metering privacy has tremendously increased over the last few years, starting out back in around 2010 with papers pointing out the privacy problems introduced by smart metering [BSU10]. Complete overviews can be found in [AY16b], [Col16], and [Wan17].

Proposals for privacy protection in smart metering can be classified according to the technique employed for providing privacy. There exist three main techniques:

- *Anonymization:* Data are transmitted so that the link between electricity readings and the identity of customers is removed [BSU10, EK10, Pet10].

- *Perturbation:* Each reading is transmitted after adding some random noise to it. Such solutions have to be tuned to provide an appropriate trade-off between privacy and accuracy [BSU10, JK12].

- *Data aggregation:* Smart meters are partitioned into communities that aggregate (add) their readings prior to transmitting them to the energy supplier. Data can be aggregated by a trusted party [DFKZB13] or making use of the homomorphic property of some cryptosystems [GJ11, KDK11, VUWS12]. The latter solutions require the use of secure computation techniques when some of the participants in the system may act dishonestly.

Finster and Baumgart [FB13] propose a system based on anonymization. It employs an anonymous peer-to-peer overlay network in its smart metering architecture. Each smart meter is in possession of a pseudonymous public key that has been previously anonymously certified by the grid operator. The smart meter then encrypts its meter reading value with the grid operator's public key and signs it with its private key. The value is then sent—together with the certificate—to the energy supplier over the overlay network.

Efthymiou and Kalogridis [EK10] propose that each smart meter should have a high-frequency identity used for anonymous transmission of meter readings on a regular basis and another low-frequency identity that is used by the smart meter for transmissions of bills, computed on the smart meter based on the readings, to the electricity supplier in infrequent intervals. The relationship between those two identities is not known by the energy supplier, but only by an escrow party.

The proposal we are presenting provides privacy by means of data aggregation employing an additive homomorphic cryptosystem. Below, we review some proposals using that approach.

García and Jacobs [GJ11] were among the first to propose a privacy-friendly smart metering architecture based on additive homomorphic encryption. In their architecture, they consider a neighbourhood with n smart meters. Each meter M_i, $i \in \{1, \ldots, n\}$ divides its energy reading m_i into n shares, m_{ij}, $j \in \{1, \ldots, n\}$, then encrypts each share m_{ij}, for $j \neq i$, under M_j's public key and sends the resulting ciphertexts to its substation SSt. Next, SSt homomorphically aggregates all $n-1$ shares encrypted under the public key of M_i and sends it the result. Each M_i decrypts the ciphertext received and adds m_{ii} to it. Finally, it sends the result to SSt. The SSt computes the aggregated energy consumption by adding all the results received. In [GJ11], each reading period requires the transmission of $O(n^2)$ ciphertexts.

Li et al. [LLL10] and Lu et al. [LLL+12] present aggregating methods that preserve customers' privacy, but they only provide security against honest-but-curious attackers.

Vetter et al. [VUWS12] suggest an approach that enables flexible server-side aggregation of smart meter readings, and combines homomorphic encryption with homomorphic message authentication codes.

Gómez Mármol et al. [GMSP+13] propose an architecture that allows the transmission of current electricity measurements to energy suppliers on a group basis, i.e. the data of individual users belonging to a group are *not* revealed in their approach. The solution is based on an additively homomorphic encryption scheme by Castelluccia et al. [CMT05]. No trusted third party is needed, but only an untrustworthy aggregating node. Each smart meter encrypts its meter value with a homomorphic key. The encrypted meter value is then forwarded to the energy supplier. However, this value cannot be decrypted

by the supplier since she is not in possession of the corresponding key. At this point, key aggregation comes into play. Each smart meter sends its homomorphic key to the aggregating node, which then aggregates all the individual keys received and forwards only the aggregated key to the energy supplier. The energy supplier can now decrypt the aggregation of the *encrypted* meter readings with the aggregated key. The proposal [GMSP+13] presents some drawbacks, such as the high complexity due to the need for smart meters to implement TLS connections, group signatures and the use of anonymous credentials.

Other aggregating systems are presented in [KDK11] and [ÁC11], but they are computationally expensive.

One problem inherent in all the approaches, especially those based on homomorphic encryption, is that checking whether the transmitted meter readings are correct (or even fall within a range of values that makes sense) is not possible for the aggregating party. There are approaches, though, that enable the party that provides the electricity to check whether the aggregation of meter readings received equals the electricity supplied, as we do in the current proposal.

García's protocol [GJ11] has $O(n^2)$ cost, with n being the number of meters per group. We present a more efficient system, whose cost is reduced to $O(n)$, based on the use of an n-out-of-n threshold ElGamal cryptosystem. A "neighbourhood" public key, whose secret key is shared among the smart meters, is used to encrypt the consumption values. Then, they are sent to a substation SSt which homomorphically aggregates them and returns the aggregated ciphertext to each smart meter. Afterwards, each smart meter computes a partial decryption using its secret key share and returns the result to the substation which will compute the cleartext aggregated value.

Our proposal makes use of a modified ElGamal in which electricity readings are encrypted after masking them with random noise. The added noise is later removed when the partial decryption is computed. This construction preserves the privacy of smart meters against a misbehaving substation.

Similarly to [DFKZB13], we use an aggregating entity, but in our case we do not need this entity to be trusted, since our system is secure against misbehaving substations, as shown in Section 4.3.

When compared to [GMSP+13], our proposal requires neither an anonymous channel, nor group signatures nor secure channels (provided, for instance, by TLS).

4.2 Efficient homomorphic smart metering proposal

Consider a neighbourhood of n smart meters M_i, $i \in \{1, \ldots, n\}$ and an electricity supplier substation SSt. Smart meters periodically send electricity measurements to SSt. We assume that each smart meter has the ability to perform basic ElGamal encryption operations. It comes with trusted hardware (like a smart card) in which the vendor has stored the parameters of an ElGamal cryptosystem (primes p, q and a group generator g). Each smart meter in the neighbourhood receives the same parameters. Each smart meter M_i also stores a secret key x_i and the corresponding public key y_i together with a certificate $Cert_i$ linking that public key with the identifier of that smart meter (it could be its serial number, for example). The authority public key required to verify $Cert_i$ is also stored in the smart card.

The proposal is performed in two stages: system set-up and electricity consumption transmission. An overall sketch of the protocol is depicted in Figure 4.2.

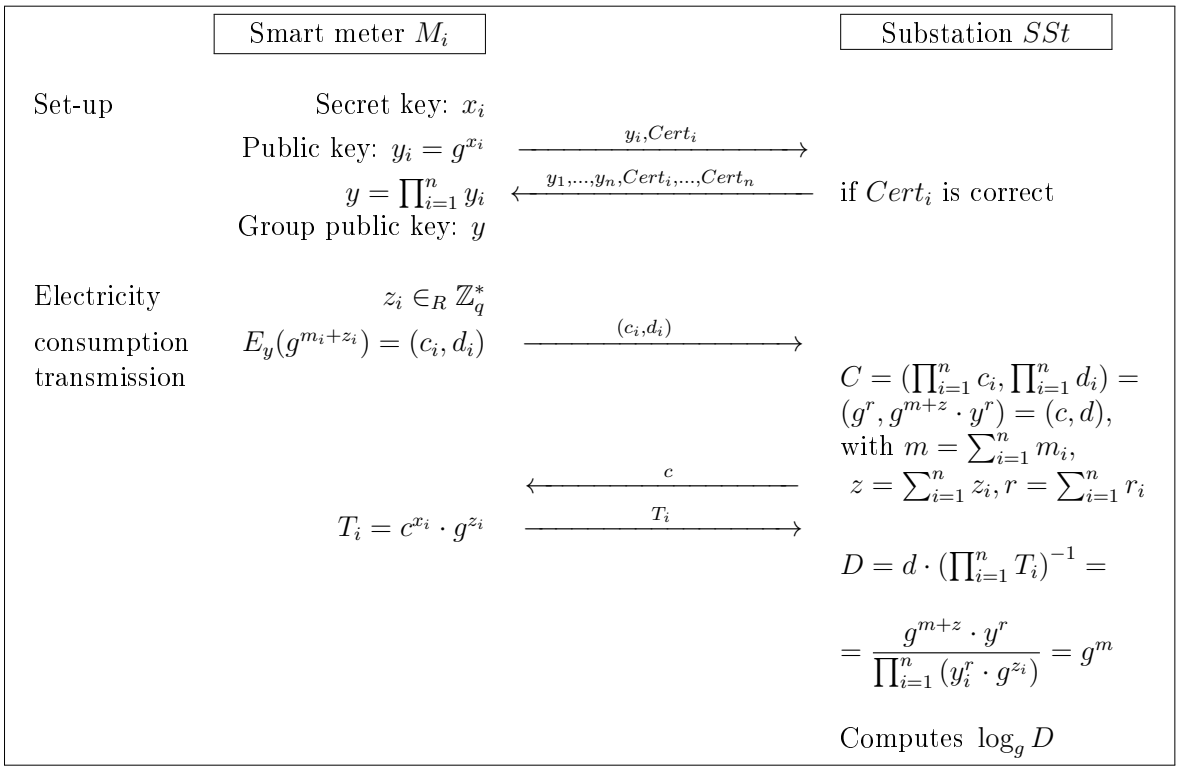


Figure 4.2: Sketch of the protocol

4.2.1 System set-up

When a smart meter is installed in a home, it establishes a connection with the SSt. Prior to transmitting electricity measurements, the SSt indicates the beginning of a key establishment operation to all the smart meters. This is done as follows:

1. SSt sends a message to each M_i indicating that a key establishment is going to be performed.
2. Each M_i sends y_i and $Cert_i$ to SSt.
3. Then SSt verifies the validity of $Cert_i$. If it is found to be correct, y_i and $Cert_i$ are sent to all the other smart meters that will perform the same verification.
4. Finally, each smart meter computes the group public key as

$$y = \prod_{i=1}^{n} y_i.$$

For privacy preservation, a smart meter will not transmit its measurements unless the number of smart meters in its group is larger than some fixed value.

4.2.2 Electricity consumption transmission

Every time period (e.g. every 30 minutes) the smart meters send their own electricity consumption to SSt. Let m_i denote the reading of smart meter M_i.

1. The SSt sends a message to each smart meter requesting its electricity measurement.

2. Each M_i generates a random noise value $z_i \in \mathbb{Z}_q^*$ and computes a ciphertext as

$$C_i = E_y\left(g^{m_i+z_i}\right) = (c_i, d_i)$$

which is sent to SSt.

3. SSt aggregates all the messages as

$$C = \left(\prod_{i=1}^{n} c_i, \prod_{i=1}^{n} d_i\right) = (c, d)$$

and sends c to each M_i.

4. Each M_i computes $T_i = c^{x_i} \cdot g^{z_i}$ and sends it to the SSt.

5. Then, SSt computes $D = d \cdot (\prod_{i=1}^{n} T_i)^{-1}$.

6. Finally, SSt computes $\log_g D$, obtaining $\sum_{i=1}^{n} m_i = m$ as a result.

Note that since m is a small number the DLP can be solved in a short time, as shown in Subsection 2.2.3.

The following lemma proves the correctness of the protocol:

Lemma 1. *If all the parties act honestly, at Step 6 the SSt obtains the addition of electricity consumptions in the neighbourhood, that is* $\sum_{i=1}^{n} m_i$.

Proof. During the electricity consumption transmission, the meters and the SSt compute the following values:

Firstly, each M_i encrypts its consumption masked with a random value.

$$C_i = E_y\left(g^{m_i+z_i}\right) = \left(g^{r_i}, g^{m_i+z_i} \cdot y^{r_i}\right)$$

Then, SSt aggregates these values as follows:

$$\begin{aligned} C &= \left(\prod_{i=1}^{n} g^{r_i}, \prod_{i=1}^{n} g^{m_i+z_i} \cdot y^{r_i}\right) = \left(g^{\sum_{i=1}^{n} r_i}, g^{(\sum_{i=1}^{n} m_i)+(\sum_{i=1}^{n} z_i)} \cdot y^{\sum_{i=1}^{n} r_i}\right) \\ &= (g^r, g^{m+z} \cdot y^r) = (c, d), \end{aligned}$$

with $r = \sum_{i=1}^{n} r_i$, $m = \sum_{i=1}^{n} m_i$, $z = \sum_{i=1}^{n} z_i$ Each smart meter computes a partial decryption T_i using its own secret key x_i:

$$T_i = c^{x_i} \cdot g^{z_i} = (g^r)^{x_i} \cdot g^{z_i} = (g^{x_i})^r \cdot g^{z_i} = y_i^r \cdot g^{z_i}$$

Finally, SSt computes:

$$D = d \cdot \left(\prod_{i=1}^{n} T_i\right)^{-1} = \frac{g^{m+z} \cdot y^r}{\prod_{i=1}^{n} (y_i^r \cdot g^{z_i})} = \frac{g^{m+z} \cdot y^r}{(\prod_{i=1}^{n} y_i^r) \cdot g^z} = \frac{g^{m+z} \cdot y^r}{g^z \cdot y^r} = g^m$$

Therefore, the aggregation of the consumptions can be obtained, as stated.

□

4.3 Security model

The main security goal of this protocol is to protect the individual consumptions in order to prevent leakage of privacy and monitoring of customers' behaviour.

In the security model, we assume that each meter acts honestly. They are tamper-resistant devices provided by the energy supplier, which periodically checks the correct maintenance of the overall installation.

Furthermore, if an honest meter is replaced with a dishonest one, the latter will not be able to send the correct certificate $Cert_i$ and it will be detected.

Then, according to [Dim14], adversaries can be classified into two main groups: honest-but-curious and malicious adversaries. The former do not interfere with the protocol but can collude in order to obtain as much information as possible. In our case, since the individual consumptions are sent encrypted using an ElGamal cryptosystem, these values cannot be disclosed to any eavesdropper.

Malicious adversaries try to make the protocol fail by providing wrong information or by interrupting the data flow.

Let us assume that the adversary *Adv* tries to impersonate the behaviour of the *SSt*. Its goal is to obtain partial aggregations of individual consumptions.

The following results show that such an adversary would not be successful.

Lemma 2. *Let $y = g^x$ be an ElGamal public key and $E_y(m) = (g^r, m \cdot y^r) = (c, d)$ be an ElGamal ciphertext (r is not known). Given a value T of the form $T = c^x \cdot g^z$, for some $z \in \mathbb{Z}_q^*$ (neither x nor z are known) obtaining m is as hard as solving the CDH problem.*

Proof. Let us assume there exists an algorithm $\mathscr{A}$ that takes g, y, $E_y(m)$ and T as input and generates m as output. Given $y = g^x$ and g^r (x and r are unknown), the value $g^{r \cdot x}$ (CDH problem) could be computed as follows:

First, compose an ElGamal ciphertext $E = (c', d')$, taking $d' \in \langle g \rangle$ at random and setting $c' = g^r$, where g is a generator of the group $\langle g \rangle$. Next, call $\mathscr{A}$ providing g, y, E and some random value $T \in \langle g \rangle$ as input and let m' be the result returned. E being an encryption of m' under public key y implies that $d' = m' \cdot y^r$. Hence, $g^{r \cdot x} = y^r$ can be obtained by simply computing $d' \cdot (m')^{-1}$.

Note that, since $T \in \langle g \rangle$, then $T \cdot ((c')^x)^{-1} \in \langle g \rangle$ and therefore there exists some value z for which $g^z = T \cdot ((c')^x)^{-1} \in \langle g \rangle$. Hence, T is of the form $(c')^x \cdot g^z$. □

From this lemma, we can prove that the adversary *Adv* cannot gain any partial aggregation of the consumption values.

Proposition 3. *Obtaining $m_2 + \ldots + m_n$ from the SSt view is as hard as solving the CDH problem.*

Proof. Let $M_1, \ldots, M_n$ be a set of smart meters that act honestly. When their measurements are requested, they transmit $E_y(g^{m_1+z_1})$, ... and $E_y(g^{m_n+z_n})$ as a response.

Let us assume that the *SSt* just aggregates the ciphertexts of $M_2, \ldots, M_n$, hence obtaining

$$C' = E_y(g^{(m_2+\ldots+m_n)+(z_2+\ldots+z_n)}) =$$
$$= (g^{r'}, g^{(m_2+\ldots+m_n)+(z_2+\ldots+z_n)} y^{r'}) = (c', d'),$$

for some unknown integer r'. Next, the *SSt* sends c' to each M_i which returns

$$T_i' = (c')^{x_i} \cdot g^{z_i}.$$

By computing $D' = \dfrac{d'}{T'_2 \cdots T'_n}$, we can see that (c', D') is an ElGamal encryption $E_{y_1}(g^{m_2+\ldots+m_n})$ encrypted under the public key of M_1. From the previous lemma, obtaining the cleartext $g^{m_2+\ldots+m_n}$ from $T_1 = (c')^{x_1} \cdot g^{z_1}$ is as hard as solving the CDH problem, hence, it is computationally unfeasible. □

Note that $E_y(g^{m_1+z_1})$ does not provide any information on z_1 since both m_1 and z_1 are unknown. Indeed, for any value z'_1 there exists an m'_1 so that $m'_1 + z'_1 = m_1 + z_1 \pmod{q}$.

4.4 Computational results

Nowadays, the Discrete Logarithm Problem is considered computationally unfeasible when using 2 048-bit exponents. In this proposal, solving a discrete logarithm is required. However, since the exponents are toy numbers, this computation turns out to be straightforward.

Indeed, according to [Ibe14], the range of the contracted capacity power in households in Spain is 0.330-14.490 KW. If the measurements are sent every 30 minutes, the consumption is 0-7.5 KWh. Note that these are the tiny values to be obtained when computing the discrete logarithm.

We performed 200 iterations of instances like this in order to check how long it takes to solve them. We represented the consumption as integers (0-7500 Wh), and thus, 13-bit numbers. Solving 200 DLP of 13-bit numbers in Sage [Dev15] using a brute force algorithm took 49.45 seconds, which means that we need 0.24725 seconds to solve just one instance of this problem when the values are so small.

Furthermore, unlike previous proposals, in this protocol we do not require communication between smart meters. Hence, the computational cost of the overall protocol is linear on the number of smart meters, $O(n)$, instead of $O(n^2)$.

– Vrai ou faux, ce qu'on dit des hommes tient souvent autant de place dans leur vie et souvent dans leur destinée que ce qu'ils font.[a]

Victor Hugo, Les Misérables

[a] Whether true or false, what is said about men often has as much influence on their lives, and particularly on their destinies, as what they do.

5 Reputation systems

This chapter focuses on reputation systems. It provides a non-exhaustive classification of commercial reputation systems, including an enumeration of the security properties that should be provided by such platforms. Academic proposals are also surveyed. Our proposal, published in the Journal of Network and Computer Applications [BPS+17], is explained in detail and analysed.

A major difficulty for Internet business in comparison to the traditional economy is the establishment of trust in potential transaction partners. Traditionally, trust has been established by word of mouth, or by surrogates such as the visual impression. These mechanisms are not available online, so a suitable replacement had to be found and *reputation systems* filled the gap. According to Resnick et al. [RKZF00], a reputation system "collects, distributes, and aggregates feedback about participants' past behaviour". While reputation systems such as the one used by eBay have been around for more than a decade, a number of theoretical and practical issues remain. One major issue is the threat to privacy [SG11, Vos04]: the history of a user's ratings reveals her preferences, which may in some cases be sensitive information.

In terms of privacy protection, if ratings are shown together with the raters' real names, anybody can simply find out, for example, in which hotels users have stayed in. Hence, travelling profiles of customers can be built, attempting against their privacy. The argument for the disclosure of real names is that trust can be built into ratings—and, thus, the reputation value of a hotel—to a certain extent, if ratings can be related to (supposed) real customers. Anonymous ratings, on the other hand, are prone to attacks in which an entity is rated multiple times by the same person (the so–called Sybil attacks [Dou02]). Cryptographic solutions can help to find a balance between anonymity and accountability, making reputation systems more attractive and reliable in practice.

Current platforms are reluctant to add privacy protection mechanisms for several reasons. First of all, many platforms make a profit by analysing customers' personal data and by personalising advertising. Secondly, the use of cryptography requires the inclusion

of cryptographic modules which increase the system complexity and development costs. Last but not least, most users do not demand privacy protection from such platforms. It is well-known that very few people read the terms and conditions section prior to creating an account[1]. Those users that do not agree with such terms have no alternative but to give up using the system.

For the sake of preserving individual rights, governments should encourage companies to implement ethical privacy-friendly systems. In this sense, the proposal presented in this thesis suggests a reputation system providing both anonymity and the opportunity to build up reputation as a rater. We focus on the example of the travel sector, as the use of reputation systems has been popular in that field for a long time. Especially online booking portals for hotels make use of reputation systems: after their stay, customers are sent an email that entitles them to rate the hotel they have stayed in. This helps other (potential) customers to decide beforehand whether they really want to stay in the hotel, based on others' experience.

On the other hand, users might not see an advantage in taking the time to rate a hotel after having finished their holiday/business trip. Why should customers take the time to fill in rating forms after their stay if they obtain no benefit from that? Some online portals have identified that problem and have introduced rewards (for example in the form of points/miles, etc.) for customers who rate hotels after their stay. Farmer and Glass [FG10] explain that there exist three main different motivations for people to collaborate:

- Altruistic motivation: the users feel an internal obligation to share. They do not do this in order to gain a reward.
- Commercial motivation: the motivation is money in the form of discounts or other kinds of rewards.
- Egocentric motivation: people collaborate because they receive recognition incentives, such as badges, and they can show off their accomplishments.

The system presented in Section 5.2 relies on commercial motivation. Highly endorsed users become *Premium* members. This privileged status could lead to obtaining discounts for future purchases or other kinds of benefit.

There exist a broad variety of commercial reputation systems. Hendrikx et al. [HBC15] presented a taxonomy based on the iterative methodology described in Nickerson et al. [NMVI09]. In [HBC15], commercial reputation systems are classified according to their architecture, organization and management. A brief survey of academic papers about reputation systems is also included.

In this thesis, we have classified commercial reputation systems in accordance with the type of service offered. This classification is not exhaustive, but it demonstrates that the requirements differ depending on the nature of each kind of service.

- Electronic Marketplaces: websites where users buy or sell a product. On some platforms, like *Amazon*[2], users rate the product and/or the seller; on others, like *eBay*[3], the users rate other users regarding their behaviour as buyers or sellers.
- Travelling: *TripAdvisor*[4] users can rate cities, hotels, restaurants,... and vote

[1] https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems
[2] http://www.amazon.com/
[3] http://www.ebay.com/
[4] http://www.tripadvisor.com/

whether other users' opinions are useful. By participating in the system, users can obtain incentives in the form of badges. *BlablaCar*[5] offers to users the possibility of sharing a car, so that they can travel cheaper and have company. Drivers and non-drivers are rated.

- Gaming: *Steam*[6] users can buy, play and rate games. They can also post screenshots and videos of their play sessions. Other users may endorse these ratings and media posts. *BoardGameGeek (BGG)*[7] is the biggest game database. Users can post their opinions and photos about any game, and rate others' contributions. There is also virtual currency, that users can gain for contributions or for donations to the system maintenance, then spend rewarding other users or buying badges to show personal interests.

- Professional skills: some platforms offer the possibility for users to have a public *curriculum vitae*, so that potential employers can check their skills. *ResearchGate*[8] and *LinkedIn*[9] also offer the possibility of endorsing other users' skills.

- Questions & Answers: there also exist some websites where users can post questions about a given topic and write an answer to other users' questions. The answers given can then be rated. *Stack Overflow*[10] is for programming and has more than 4 million registered users.

The first three types can easily be compared to a platform for booking and rating hotels. Below, the most desirable properties for such services are listed.

P1. Users can only write comments about products they have tested before, i.e. hotels they have stayed in.

P2. Comments are anonymous and unlinkable.

P3. Users can endorse any comment.

P4. A user can endorse a given comment at most once.

P5. Endorsements are anonymous.

P6. Users obtain some kind of reward for posting useful comments.

P7. Endorsement correctness can be verified.

Next, in Table 5.1 it is analysed whether these properties are fulfilled by such platforms (✓) or not (·), or are not applicable (N.A.).

In this table it can easily be seen that our system is the only one meeting P2 and P7, while P6 is given by almost all the platforms. The fact that a given property is not implemented may just mean that it is not relevant for the platform interests or may require a lot of resources. Platforms may not be interested in comments being anonymous

[5] https://www.blablacar.com/
[6] http://store.steampowered.com/
[7] https://boardgamegeek.com/
[8] http://www.researchgate.net/
[9] https://www.linkedin.com
[10] https://stackoverflow.com/

Platforms	P1	P2	P3	P4	P5	P6	P7
Amazon	·	·	✓	✓	✓	✓	·
eBay	·	·	·	N.A.	N.A.	✓	N.A.
TripAdvisor	·	·	✓	·	✓	✓	·
BlablaCar	✓	·	·	N.A.	N.A.	✓	N.A.
Steam	✓	·	✓	✓	✓	·	·
BGG	·	·	✓	✓	·	✓	·
Ours	✓	✓	✓	✓	✓	✓	✓

Table 5.1: Commercial reputation systems and their security properties

(P2), since in this way customers are able to find out what other customers bought and this might result in more purchases. Endorsement correctness (P7) is, in most cases, not an interesting property, since it does not have a direct effect on the platform's profit. User rewards (P6) are the usual way to attract customer attention.

5.1 Related work

Early approaches to introduce privacy protection in reputation systems, like the one by Steinbrecher [Ste06], for example, were based on the usage of pseudonyms instead of users' real names. However, such approaches still allow for a linkage of all the ratings performed by a user, under the pseudonym. Even though one might think that user's privacy is protected, as the profile under the pseudonym cannot be linked to an individual (directly), this is not the case, as Narayanan et al. [NS08] have pointed out. In particular, they managed to de-anonymize the movie ratings of 500,000 subscribers of *Netflix* given only a small amount of background knowledge about individual users (from the *Internet Movie Database*). Thus, profiles under a pseudonym should be considered as being prone to de-anonymization attacks and reputation systems based on basic pseudonymization cannot be considered to sufficiently protect users' privacy.

Schaub et al. [SBHB16] propose a reputation system in which customers can issue anonymous and unlinkable comments about service providers with which they have interacted. In their proposal, a service provider issues the credentials through which customers can rate it. That makes the system prone to attacks in which a malicious service provider makes use of self-made credentials to issue positive ratings about itself (ballot stuffing attack). The authors refer to that vulnerability and mention that a solution based on the use of electronic coins could partially mitigate the problem.

Blömer et al. [BJK15] present a construction of a reputation system based on group signatures. In their proposal, customers are allowed to rate products they have purchased previously by generating an anonymous signed message. If a customer rates a product more than once, her anonymity will be lifted.

Kerschbaum [Ker09] and Petrlic et al. [PLS14] have come up with approaches for reputation systems that meet strong privacy guarantees. The approaches are based on homomorphic encryption and no one retrieves any individual ratings by users but only the aggregation of a number of individual ratings – i.e. the reputation value – can be retrieved.

However, strong privacy protection in reputation systems hinders the implementation of mechanisms that allow users to become experts if they contribute with good ratings. Such mechanisms can constitute good incentives for users, though, to actively participate

in the reputation system. Camenisch et al. [CGHH10] present an approach that allows for such a privacy-preserving reputation system with an incentive mechanism built into it whereby raters can gain reputation. Their approach is based on e-cash and they present *Wikipedia* as a possible platform where the approach could be useful. One of the drawbacks of their approach, though, is that the electronic coins are not linked to the users (i.e. their pseudonyms) and, thus, users can delegate their reputation gained to other users.

Kokoschka et al. [KPS15] also present an approach for a reputation system that guarantees both privacy protection for raters and provides an incentive mechanism that is based on the idea that raters can become experts if they issue a great deal of ratings. The approach protects, up to a certain extent, against attacks by raters who would just perform a huge amount of ratings in order to become experts by allowing only authorized users to rate, i.e. only users who have previously executed a transaction with the party to be rated.

The aim of this work is to come up with an anonymous reputation system which, in addition to the usual features of such a system, also allows the raters to build up reputation. While the approach can be generalized, we present it using the example of a hotel reputation system, since this is an important application domain. The benefits for users are manifold: Users might have an implicit incentive to provide useful ratings as they can then become *Premium* users. Portals like Tripadvisor have proven such an approach to be useful. At the same time, the explicit incentive to become a *Premium* user can be an economic one: *Premium* users might obtain hotel discounts in the future. Thus, the more *useful* ratings a user submits, the more she can benefit. The usefulness of ratings is determined by other customers who might have stayed in a certain hotel room based on a user's rating. One of the major advantages of this approach, compared to portals that already include it, is that our system is built in a *privacy-respecting* way.

5.2 Privacy-preserving reputation system proposal

We assume an online platform which manages hotel room reservations. The platform permits users who have been in some hotel to anonymously publish a text describing their opinion about that hotel. Opinions are public so that they can be read by other users. If some user finds that some text has been specially useful for her, she can anonymously endorse it. Users receiving a large amount of endorsements from different people (over a given threshold) become *Premium* users. This status could provide some advantages like price discounts on further reservations.

An overview of the system, its participants and protocols is given in Figure 5.1. The participants involved in this protocol are:

- Service provider SP: entity that manages the website and the cryptographic keys of the system.
- Hotels (denoted as h_i): entities offering a service through the SP.
- Users (denoted as u_j): people that book a hotel room and may comment about it. They can endorse comments made by other users.

The following requirements are met by the proposed system:

1. Users can only write comments about hotels they have stayed in.

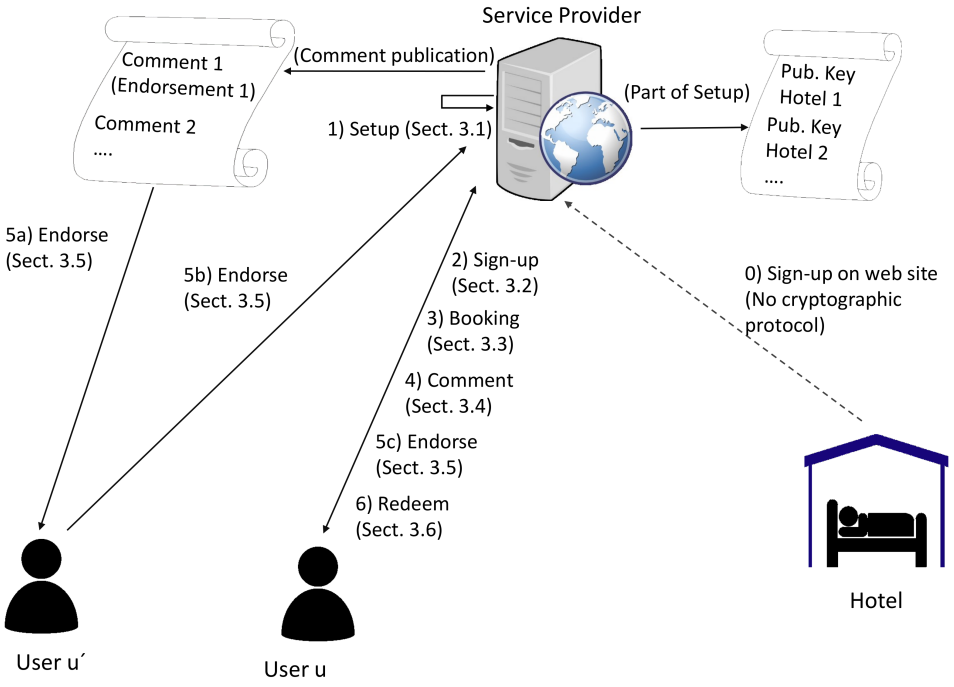


Figure 5.1: Overview of participants and protocols

2. Comments about hotels are anonymous and unlinkable.
3. Users can endorse any comment.
4. A user can endorse a given comment at most once.
5. Comment endorsements are anonymous.
6. A user becomes *Premium* after collecting a certain amount of endorsements from different people.
7. Comment endorsement correctness can be verified.

The system is composed of six protocols:

- *Set-up*: The service provider, SP, generates the system parameters. At this point, the SP establishes the amount of endorsements required to become *Premium*.
- *Sign-up*: A user creates an account in the system. As a result, she obtains the capability of endorsing other users' comments.
- *Booking*: A user with an account in the system makes (and pays for) a reservation for hotel h. After that, she obtains the capability of writing a comment about h.
- *Comment*: After staying in hotel h, a user u writes an anonymous public comment about it. This is only possible after a proper execution of the *booking* protocol.
- *Endorsement*: A user with an account can endorse a comment made by some other user.
- *Redeem*: After obtaining a certain amount of endorsements from different people, a user becomes a *Premium* user and can obtain the promised reward.

5.2.1 Set-up

The service provider SP first sets up an ElGamal cryptosystem by choosing two primes p, q, such that $q \mid p-1$, and a generator g, so that $G = \langle g \rangle$ is an order q multiplicative subgroup of $\mathbb{Z}_p$ (see Section 2.2). Then, it generates its ElGamal private/public key pair (x_{SP}, y_{SP}). As usual, the public key should be certified by some certificate authority.

For each hotel h with an account on the platform, the SP generates an ElGamal private/public key pair (x_h, y_h). The public key y_h is published on the platform linked to the profile of h through $Sign_{x_{SP}}(\text{“name-of-hotel-h”}||y_h)$, a message signed by SP. The secret key x_h is stored and kept secret by the SP.

Each time a new hotel sets up an account, the service provider generates a key pair that is linked to that hotel account.

After that, the SP generates a random secret $\sigma \in \{0, \ldots, q-1\}$ and sets the value t which corresponds to the amount of different endorsements required to become a *Premium* user. Next, it generates a set of n shares (X_i, σ_i) for σ using Feldman's t-out-of-n verifiable secret sharing scheme (see Section 2.4.2). Values $c_0, c_1, \ldots, c_{t-1}$, needed for verifiability, are made available on the platform bulletin board. The proper amount n of generated shares will be analysed in Section 5.4. For each share (X_i, σ_i), the SP generates a tuple of the form $(X_i, \sigma_i, S_i, Sign_{x_{SP}}(X_i||S_i))$, with $S_i = g^{\sigma_i}$.

A summary of the parameters generated in this step can be seen in Figure 5.2.

Service provider SP
SP's key pair: (x_{SP}, y_{SP})
A key pair for each hotel h_j : (x_{h_j}, y_{h_j})
Secret: σ
Threshold: t
n shares: (X_i, σ_i)
Verification values: $c_0, c_1, \ldots, c_{t-1}$

Figure 5.2: Parameters generated in the set-up stage

5.2.2 Sign-up

Before a user u is able to use the system, she has to sign up to the system. When she signs up, she gives her name (together with some additional data such as her address, phone number, etc.) and a credit card number. At this point, u has to prove that she is the owner of that credit card. This can be done, for instance, by asking her to make a small payment that will be refunded later. The SP stores her data and the hash of the credit card number provided.

The credit card number is required as a measure to prevent dishonest users from creating a large amount of accounts (Sybil attack). Each time an account is created, the SP checks whether the hash number of the card provided has been stored associated with a previous account. In this way, a dishonest user's capacity to create more than one account is limited by the amount of cards she is in possession of. It has been proven that a trusted central authority issuing unique credentials to an actual human being is the only method that may eliminate Sybil attacks completely [Dou02]. Unfortunately, that measure would prevent people without a certificate from using the system. See [BS12] for a complete survey about measures against the Sybil attack.

The following steps are performed during the sign-up process (after checking u's credit card):

- User u contacts the SP and engages a 1-out-of-n oblivious transfer protocol with it (see Section 2.5). After running this protocol, she obliviously receives one of the tuples $(X_i, \sigma_i, S_i, Sign_{x_{SP}}(X_i||S_i))$, for some index $i \in \{1, \ldots, n\}$. The SP does not know which of the n tuples has been actually transferred.

  The tuple received and stored by user u will be denoted

  $$(X_u, \sigma_u, S_u, Sign_{x_{SP}}(X_u||S_u)).$$

  This tuple consists of a fragment of the secret σ together with some information required for verifiability. User u will use this tuple to endorse other users' comments. Note that different users could receive the same tuple. This is discussed in Section 5.4.

- User u verifies the tuple received by checking $S_u = g^{\sigma_u}$, the signature by SP on $X_u||S_u$ and, then, she verifies the secret share received by checking whether it fulfils:

  $$S_u \stackrel{?}{=} \prod_{j=0}^{t-1} (c_j)^{{X_u}^j}.$$

- User u generates an element $g_u \in_R G$, by choosing a random seed $seed_u$ and computing $g_u = \mathscr{H}(seed_u)$. The hash function $\mathscr{H}$ must ensure that $\log_g(g_u)$ is kept unknown. This element will be used to receive endorsements. User u will become *Premium* if she manages to obtain g_u^{σ}. User u stores $seed_u$ and g_u.

A sketch of this step can be seen in Figure 5.3.

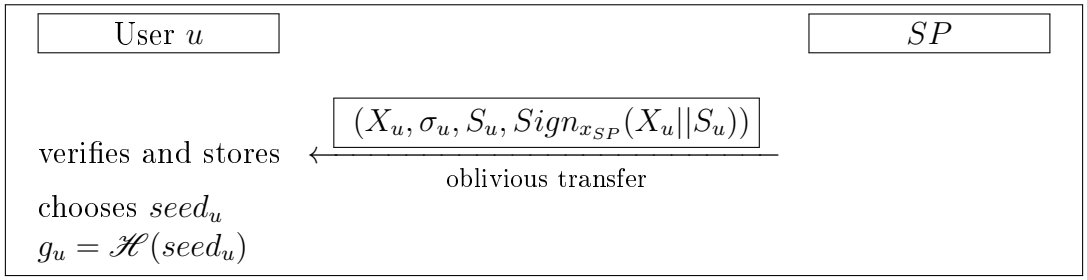


Figure 5.3: Sketch of sign-up

5.2.3 Booking

A user u makes a reservation for hotel h. The following steps are performed after u has made (and paid) a reservation for hotel h:

- User u generates an ElGamal key pair (x_{u_h}, y_{u_h}). This key pair will be used by u to sign her comment about hotel h.

- User u contacts SP and asks her to blindly sign y_{u_h} with private key x_h. As a result, she obtains a certificate $Cert_{x_h}(y_{u_h})$, which can be verified with public key y_h. Public key y_{u_h} cannot be linked to u but, by means of this anonymous certificate, it is known that it belongs to some user who made a reservation for hotel h. Hence, she can write a comment about that hotel.

This step is sketched in Figure 5.4.

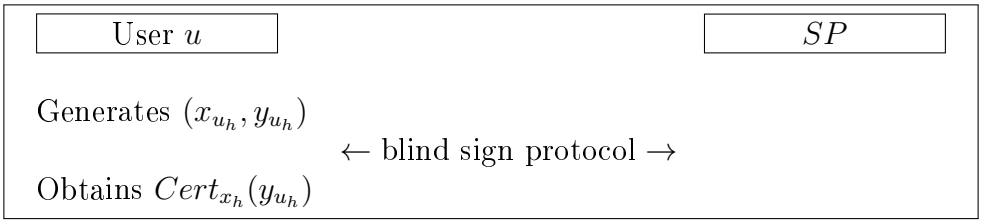


Figure 5.4: Sketch of booking

5.2.4 Comment

After visiting a hotel a user may write an assessment about her own experience in order to help other users to make a choice. If her comments are widely endorsed, she will become a *Premium* user.

In order to post a comment about hotel h, the user u has to publish the following items:

- The assessment m with her opinion about hotel h.
- A value $G_{u,r} = g_u^r$, masks g_u with a random $r \in_R \{1, \ldots, q-1\}$. User u has to store the value r.
- The signature on $m||G_{u,r}$ computed with private key x_{u_h} and verifiable with public key y_{u_h}, that is $Sign_{x_{u_h}}(m||G_{u,r})$.
- The certificate $Cert_{x_h}(y_{u_h})$.

The platform, prior to publishing a comment, will check the validity of $Cert_{x_h}(y_{u_h})$ and the signature on $m||G_{u,r}$. Hence, the SP checks that the comment has been issued by a user that has performed a booking for hotel h. Any user can perform the same verification.

All the comments about h signed with y_{u_h} are anonymous but linkable among them (their signature is verifiable under the same public key). Comments made after different reservations are not linkable since each time a user makes a reservation for hotel h, she obtains a different signed public key. Hence, linkability is avoided as long as users do not pose more than one comment after each reservation.

The structure of a comment by user u about hotel h can be seen in Figure 5.5.

5.2.5 Endorsement

When some user u' with a tuple $(X_{u'}, \sigma_{u'}, S_{u'}, Sign_{x_{SP}}(X_{u'}||S_{u'}))$ concludes that a comment written by some other user u (whose identity she does not know) has been useful for her, she may endorse it.

The endorsement protocol proceeds as follows:

m	Opinion about hotel h
$G_{u,r}$	"Identifier" g_u masked with random r
$Sign_{x_{u_h}}(m\|\|G_{u,r})$	Signature of m linked to $G_{u,r}$
$Cert_{x_h}(y_{u_h})$	Certificate of u's public key for hotel h

Figure 5.5: Structure of a comment of hotel h by user u

- User u' takes the value $G_{u,r}$ from u's comment and computes $(G_{u,r})^{\sigma_{u'}}$.
- User u' sends $((G_{u,r})^{\sigma_{u'}}, X_{u'}, S_{u'}, Sign_{x_{SP}}(X_{u'}||S_{u'}))$ to the platform, together with a Chaum-Pedersen proof $CP(G_{u,r}, g, (G_{u,r})^{\sigma_{u'}}, S_{u'})$.
- The platform checks the signature $Sign_{x_{SP}}(X_{u'}||S_{u'}))$ and the correctness of $CP(G_{u,r}, g, (G_{u,r})^{\sigma_{u'}}, S_{u'})$.

  If it does not fulfil the previous verification, the endorsement is rejected and the protocol ends here. Otherwise, the platform makes that data available. When user u notices that one of her comments has been endorsed, she will proceed as follows:
- User u performs the previous verification and then computes $((G_{u,r})^{\sigma_{u'}})^{-r} = (g_u)^{\sigma_{u'}}$.
- User u stores $(X_{u'}, (g_u)^{\sigma_{u'}})$.

A sketch of this step can be seen in Figure 5.6.

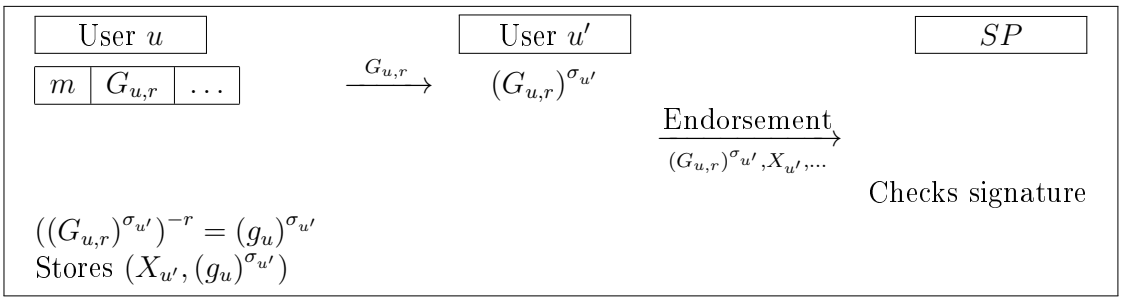


Figure 5.6: Sketch of endorsement

5.2.6 Redeem

When the amount of endorsements received by user u reaches the threshold t, she becomes *Premium*. This is performed as follows:

- User u computes:

$$G_u = \prod_{i=0}^{t} ((g_u)^{\sigma_i})^{\lambda_i} .$$

  Note that $G_u = g_u^{\sigma}$.
- User u sends $seed_u$ and G_u to the SP.
- The SP computes $g_u = \mathscr{H}(seed_u)$ and checks $G_u = g_u^{\sigma}$.
- The SP updates u's status to *Premium*.

A sketch of this step can be seen in Figure 5.7. A summary of the most important parameters generated during the protocol and their purpose are shown in Figure 5.8.

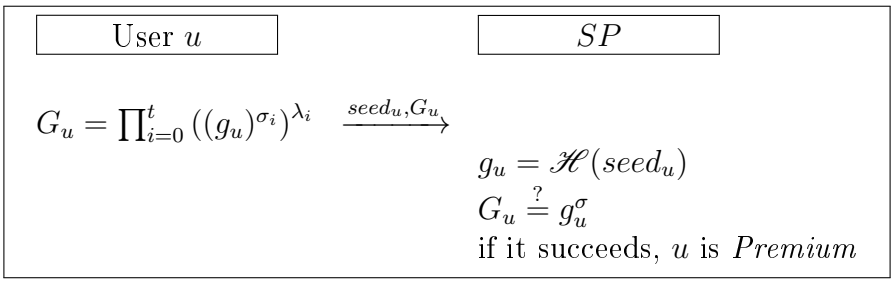


Figure 5.7: Sketch of redeem

Parameter	Purpose	Used by
(X_u, σ_u)	A share to endorse other users' comments. S_u and $Sign_{x_{SP}}(X_u \|\| S_u)$ are for verifications.	User u
g_u	An "identifier" for receiving endorsements.	
(x_{u_h}, y_{u_h})	A key pair for each hotel visited. A comment about hotel h is signed with x_{u_h}.	
(x_{SP}, y_{SP})	Key pair for signing shares.	SP
(x_h, y_h)	u generates a key pair for each hotel visited. Her public key y_{u_h} is certified by SP by signing it with x_h.	

Figure 5.8: Summary of the parameters of the system

5.3 Security analysis

In this section the fulfilment of the security requirements claimed is analysed. Before that, the security assumptions are detailed. That is, the assumed *attacker model* is described as follows:

- The service provider, SP, is a trusted party. It will follow all protocols properly and will not reveal information which can jeopardize users' privacy. Users trust it to manage their hotel reservations, so that it is aware of all users' reservations. Nevertheless, users do not want it to be aware of their opinions.

- Users are not trusted. Some of them may cheat so as to become *Premium* without having achieved the necessary requirements. Others may also be interested in tracing other users' opinions and preferences. Some others may post bad comments on purpose to hinder competitors.

The following requirements are met by the proposed system:

1. *Users can only write comments about hotels they have stayed in.*
   A comment about hotel h written by user u is only accepted if it includes a digital signature verifiable with a public key y_{u_h} which has been (blindly) signed by the SP and its signature is verifiable with y_h. The SP will only sign such a key with private key x_h after user u has made and paid for a reservation for hotel h.

2. *Comments about hotels are anonymous and unlinkable.*
   A comment by user u includes the assessment m, a value $G_{u,r}$, a digital signature $Sign_{x_{u_h}}(m \|\| G_{u,r})$ and a certificate $Cert_{x_h}(y_{u_h})$.

The assessment m is a text message written by u. It cannot be related to u unless it includes some self-reference. User u, wishing to preserve her anonymity, would not include such references in m.

The value $G_{u,r}$ is computed as $G_{u,r} = g_u^r$ for some random r. Since r is kept secret by u and is never revealed, $G_{u,r}$ and g_u cannot be linked (assuming the intractability of the DLP). Moreover, the value r can be chosen to be different for each of the comments posted by u, so that values $G_{u,r}$ and $G_{u,r'}$ being part of different comments, are not linkable.

Regarding the public key y_{u_h}, it has been privately generated by u and its certificate $Cert_{x_h}(x_{u_h})$ by the SP has been obtained blindly. Hence, not even the SP, which signed it, can relate it to u.

As mentioned in Section 5.2.4, different comments signed under the same key y_{u_h} remain anonymous but are known to have been posted by the same user. Unlinkability is provided as long as each key y_{u_h} is not used more than once.

3. *Users can endorse any comment.*
When a user u' creates an account for the first time, she receives a tuple $(X_{u'}, \sigma_{u'}, S_{u'}, Sign_{x_{SP}}(X_{u'}||S_{u'}))$. In order to endorse a comment m of some other user u, she has to take the value $G_{u,r}$, which is published together with m, compute $(G_{u,r})^{\sigma_{u'}}$ and publish the result obtained. Hence, possession of such a tuple permits an endorsement operation to be carried out.

4. *A given user can endorse a given comment once at most.*
Assuming that the measures against the Sybil attack implemented by the platform are effective, no user u' can create more than one account in the system. Thus, she will only have one tuple $(X_{u'}, \sigma_{u'}, S_{u'}, Sign_{x_{SP}}(X_{u'}||S_{u'}))$. If u' endorses a comment m more than once, she will generate the same value $(G_{u,r})^{\sigma_{u'}}$ every time. This situation is easy to detect. Moreover, duplicate endorsements do not provide information helping u to become a *Premium* user.

5. *Comment endorsements are anonymous.*
A given user u' endorses other users' comments by making use of the tuple $(X_{u'}, \sigma_{u'}, S_{u'}, Sign_{x_{SP}}(X_{u'}||S_{u'}))$. This tuple is obtained by u' through an oblivious transfer protocol. Hence, nobody can know which of the n tuples was actually received by u'. Hence, her endorsements are anonymous.

6. *A user becomes* Premium *after collecting t endorsements from different people.*
When user u has collected t endorsements from different people, she has t pairs of the form $(X_i, (g_u)^{\sigma_i})$ with all the X_i components being different. Then, she is able to compute $G_u = g_u^{\sigma}$. Upon receiving this value (and with the corresponding verifications succeeding), the SP will set her status to *Premium*. The value G_u does not provide any information about the pairs $(X_i, (g_u)^{\sigma_i})$ from which it has been obtained. Hence, the redeem protocol has no risk for privacy.

   The use of the hash function $\mathscr{H}$ assures that g_u cannot be generated in an arbitrary way. If a user knows the discrete logarithm relation existing between two or more g_{u_i}, then she can generate as many *Premium* accounts as she wishes, without following the protocol. That is, given $g_{u_1}, g_{u_2} = (g_{u_1})^k$, for some integer k, she can easily compute $g_{u_2}^{\sigma}$ from $g_{u_1}^{\sigma}$.

7. *Comment endorsement correctness can be verified.*
   A comment endorsement $(G_{u,r})^{\sigma_{u'}}$, $X_{u'}$, $S_{u'}$, $Sign_{x_{SP}}(X_{u'}||S_{u'}))$ is sent together with a Chaum-Pedersen proof $CP(G_{u,r}, g, (G_{u,r})^{\sigma_{u'}}, S_{u'})$ to test the correctness of $(G_{u,r})^{\sigma_{u'}}$.

There exists another kind of attacks that may succeed because the users of the system have inappropriate behaviour. They are called *social attacks*. It is very difficult to avoid these attacks, since they cannot be countered purely relying on technical solutions. When a user writes a comment, she may not write the truth. Cryptography cannot avoid misuse of the system. However, the honest behaviour of a vast majority of users will lead to a system that enables useful assessments. We provide cryptographic tools that permit privacy as long as users provide honest ratings.

As a side note, the system is also easy to implement. As depicted in Figure 5.1, all interactions happen with the service provider even though we limit the information that the service provider receives. Direct communication between any other entities is not required. This simplifies the development of an app implementing our proposal. In principle, the simple communication model even allows an implementation in JavaScript, as we base our work on efficient cryptographic protocols. There are several libraries that demonstrate the feasibility of asymmetric cryptography in Javascript [JSl]. Additional security considerations would be required in this case, e.g. to ensure authenticity of the JavaScript code delivered by the service provider. A detailed analysis of these issues may be left as future work.

5.4 Generation of shares

During the set-up protocol (Subsection 5.2.1), the SP chooses a secret σ and creates a set of n shares (X_i, σ_i) for σ using a t-out-of-n secret sharing scheme. Users obliviously receive one of these shares after creating an account in the system. Consequently, the share received by a user does not depend on the shares transmitted previously to other users, and therefore a given share can be received by more than one user.

Note that, in a secret sharing scheme, a dealer could generate the shares on demand. However, in this protocol, the shares are obliviously transferred to the users at the moment they create their own account. Hence, to run the oblivious transfer protocol, the value of n has to be fixed beforehand.

During an endorsement operation, the endorsed user receives information about the share of the endorser. A user u that collects information about t *different* shares is able to compute g_u^{σ} and become *Premium*.

It could happen that a user that has collected t endorsements from t different people cannot become *Premium* because some of them are repeated and the actual amount of different shares t' is smaller than t. Below we analyse the associated probabilities.

5.4.1 Probabilities analysis

Let n be the amount of shares generated. We consider an experiment in which we randomly take a set of t, $t \ll n$, users and each of them provides her own share.

In the aforementioned experiment, let $\mathrm{RV}(n, t)$ be the random variable that returns the amount of *different shares* observed among the t that have been received. Assuming $t \ll n$, the sample space of $\mathrm{RV}(n, t)$ is $\{1, \ldots, t\}$.

The probability of $\mathrm{RV}(n,t)$ returning each value of the sample space, that is

$$\mathrm{Prob}[\mathrm{RV}(n,t) \;=\; t'],$$

for each $0 \leq t' \leq t$, can be computed by means of the following recursive statement:

- If $t' = 0$,
$$\mathrm{Prob}[\mathrm{RV}(n,t) = t'] = 0.$$
- If $t' = t$,
$$\mathrm{Prob}[\mathrm{RV}(n,t) = t'] = \frac{(n-1)}{n} \cdot \frac{(n-2)}{n} \cdots \frac{(n-t'+1)}{n}.$$
- Otherwise,
$$\begin{aligned}\mathrm{Prob}[\mathrm{RV}(n,t) = t'] \;&= \tfrac{(n-t'+1)}{n} \cdot \mathrm{Prob}[\mathrm{RV}(n,t-1) = (t'-1)] \\ &+ \tfrac{t'}{n} \cdot \mathrm{Prob}[\mathrm{RV}(n,t-1) = t')].\end{aligned}$$

5.4.2 Tuning n and t'

Let n be the amount of shares generated by the SP and let t be the amount of endorsements *from different people* required to become *Premium*. We will denote t' the actual threshold employed to set up the t'-out-of-n secret sharing scheme.

By taking an extremely large value for n and setting $t' = t$, a user collecting t endorsements would obtain all of them as different with overwhelming probability so that she would become *Premium*. That is,

$$\lim_{n\to\infty} \mathrm{Prob}[\mathrm{RV}(n,t) = t] = 1.$$

Unfortunately, a too large value for n causes elevated share generation and storage costs. Moreover, the cost of an oblivious transfer protocol also increases with n. Hence, reduced values for n are required.

As an example, by making use of the formulas in Subsection 5.4.1, we have computed, for $t' = t = 100$, the amount n of shares to be generated so that a user that has received 100 endorsements really becomes *Premium* with a probability larger than $1 - \epsilon$. That is, we have computed the minimum n, satisfying that

$$\mathrm{Prob}[\mathrm{RV}(n,t) = t] \geq (1-\epsilon).$$

The results are shown in the first row of Table 5.2. It can be seen that, in all cases, the value n is really large.

We can reduce the value of n by reducing the threshold t' so that it is slightly smaller than t. Hence, a user is asked to collect t endorsements but, to become *Premium*, just t' (all being different) are really required.

Table 5.2 shows the minimum value n satisfying

$$\mathrm{Prob}[\mathrm{RV}(n,t) \geq t'] \geq (1-\epsilon).$$

for $\epsilon = 10^{-4}$, 10^{-5} and 10^{-6}. It can be seen that more affordable values for n are obtained.

t'	$\epsilon = 10^{-4}$	$\epsilon = 10^{-5}$	$\epsilon = 10^{-6}$
100	49497559	494997559	4949997558
99	343734	1090438	3451719
98	55939	121887	263959
97	20534	37252	66972
96	10578	17227	27755
95	6508	9870	14797

Table 5.2: Number of shares n to be generated for $t = 100$ and different values for t' and ϵ.

– Wer noch nie einen Fehler gemacht hat, hat sich noch nie an etwas Neuem versucht.[a]

Albert Einstein

– I became insane, with long intervals of horrible sanity.

Edgar Allan Poe

[a] Anyone who has never made a mistake has never tried anything new.

6

Conclusions and future work

This thesis has discussed some open problems related to the privacy needs that arise from the intensive use of ICT in our society. More precisely, three new e-Services systems have been designed in order to offer new effective and privacy-preserving solutions in the e-Business field.

Firstly, a counter-based coupon system, which is an enhancement of the EFS scheme [EFS04], has been developed. The method presented is publicly verifiable and more efficient, since it permits the loyalty-points counter to be increased by k units in a single operation.

The public key list $\mathscr{L}$ is computed just once by the vendor at set-up time and posted on the public board. The utility of this list is twofold. Firstly, the customer uses it to unblind the signature whenever the loyalty-points counter is updated. Secondly, it allows two public verifications to be performed: one when the customer obtains her increased counter, and the other one to publicly check the coupon validity in the redeem stage.

In the original EFS system, the loyalty-points counter had to be increased one by one. At the redeem stage, although the vendor could also compute $x^k B_i$, the customer was not able to check its correctness. In the system presented in this thesis, this verification can be performed using the public information $\mathscr{L}$. This new feature makes this system more flexible in order to be adapted to the vendor's marketing strategies. Moreover, the use of elliptic curve cryptography permits the proposed system to be implemented on resource-constrained devices, reducing its economic cost.

Secondly, an efficient privacy-preserving system for reporting the consumption of a neighbourhood of n smart meters has been presented. By homomorphically adding all n consumptions, the existing link between a customer and her consumption is broken. In this way, the privacy of customers is preserved.

The proposed scheme does not require a trusted third party, and has a linear, $O(n)$, communication complexity. An experimental evaluation has shown that it can be feasible for realistic electricity consumption values.

The third contribution of this thesis focused on reputation systems. Indeed, while in traditional markets the buyers' confidence is built upon previous personal experience or based on word-of-mouth, in online transactions reputation systems are required to provide

trust. In our proposal, ratings are anonymous but reliable, since they are guaranteed to be posted by a user who has actually used the service before (in the example of a hotel reputation system, for instance, the user is required to have previously paid for a reservation at the rated hotel). Furthermore, good raters are promoted in order to favour useful comments. Users can endorse the ratings they found to be useful. Then, a user receiving a pre-defined number of endorsements is considered experienced and obtains *Premium* member status. Cryptographic security of the system is proven to achieve the requirements claimed.

In addition, a taxonomy of the commercial reputation systems has been sketched, according to the type of service offered. A comparison is given of desirable security properties offered by our system in relation to commercial ones. Any other system but ours provides anonymous and unlinkable comments, and endorsement correctness verifiability.

The research presented in this thesis could be taken further. Some additional tests and experiments, as well as real implementations of the proposals presented in this dissertation, could be developed. This thesis could be enhanced by addressing the following issues:

- Our loyalty system proposal could be implemented in real life and tested. First, a usability study should be carried out. Which device would be a better option for customers should be studied: mobile telephones, RFID cards or even USD drives. It would also be necessary to study how to implement its different cases of use, such as checking the points balance. This study, implementation and maintenance could lead to a business, for example, in the form of a spin-off.

- Study the amount of meters to be grouped together in order to be confident that the privacy of individual customers is preserved.

- Study additional security considerations for our reputation system and to implement it using JavaScript.

- Study the inclusion of post quantum cryptography in our proposals.

Bibliography

[ÁC11] G. Ács and C. Castelluccia. I Have a DREAM! (DiffeRentially privatE smArt Metering). In *Information hiding: 13th international conference*, pages 118–132. Springer-Verlag, Berlin, Heidelberg, 2011. 978-3-642-24178-9, 10.1007/978-3-642-24178-9_9.

[AEL+08] F. Armknecht, A.N. Escalante, H. Löhr, M. Manulis, and A. Sadeghi. Secure multi-coupons for federated environments: privacy-preserving and customer-friendly. In *Proceedings of information security practice and experience*, volume 4991 of *ISPEC'08*, pages 29–44. Springer-Verlag, Berlin, Heidelberg, 2008. 10.1007/978-3-540-79104-1_3.

[ANS12] ANSI ASC. X9.95 Standard for Trusted Time Stamps, 2012. https://goo.gl/vbevuB.

[AY16a] D. Alahakoon and X. Yu. Smart electricity meter data intelligence for future energy systems: a survey. *IEEE transactions on industrial informatics*, 12(1):425–436, 2016. 1551-3203, 10.1109/TII.2015.2414355.

[AY16b] D. Alahakoon and X. Yu. Smart electricity meter data intelligence for future energy systems: a survey. *IEEE transactions on industrial informatics*, 12(1):425–436, 2016. 1551-3203, 10.1109/TII.2015.2414355.

[Bar09] P. Barreto. The pairing-based crypto lounge, 2009. https://goo.gl/deLYK6.

[Ber13] J. Berry. Bulking up: the 2013 COLLOQUY loyalty census, 2013. https://goo.gl/Wme7J7.

[BF01] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proceedings of advances in cryptology*, CRYPTO'01, pages 213–229. Springer-Verlag, Berlin, Heidelberg, 2001. 10.1007/3-540-44647-8_13.

[BJGG+13] F. Borrego-Jaraba, P.C. Garrido, G.C. García, I.L. Ruiz, and M.Á. Gómez-Nieto. Ubiquitous NFC solution for the development of tailored marketing strategies based on discount vouchers and loyalty cards. *Sensors*, 13(5):6334–6354, 2013. 10.3390/s130506334.

[BJK15] J. Blömer, J. Juhnke, and C. Kolb. Anonymous and publicly linkable reputation systems. In *19th international conference on financial cryptography and data security*, FC'15, pages 478–488. Springer-Verlag, Berlin, Heidelberg, 2015. 978-3-662-47854-7, 10.1007/978-3-662-47854-7_29.

[BLS04] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004. 0933-2790, 10.1007/s00145-004-0314-9.

[Bol03] A. Boldyreva. Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In *Proceedings of the 6th international workshop on theory and practice in public key cryptography*, PKC'03, pages 31–46. Springer-Verlag, Berlin, Heidelberg, 2003. 10.1007/3-540-36288-6_3.

[BPS+16] N. Busom, R. Petrlic, F. Sebé, C. Sorge, and M. Valls. Efficient mart metering based on homomorphic encryption. *Computer Communications*, 82:95–101, 2016. 0140-3664, 10.1016/j.comcom.2015.08.016.

[BPS+17] N. Busom, R. Petrlic, F. Sebé, C. Sorge, and M. Valls. A privacy-preserving reputation system with user rewards. *Journal of Network and Computer Applications*, 80:58–66, 2017. 1084-8045, 10.1016/j.jnca.2016.12.023.

[BS12] N. Balachandran and S. Sanyal. A review of techniques to mitigate sybil attacks. *International journal of advanced networking & applications*, 4(1):1514–1518, 2012. 0975-0282, https://goo.gl/mkkbtv.

[BSU10] J.M. Bohli, C. Sorge, and O. Ugus. A privacy model for smart metering. In *Proceedings of the 1st IEEE international conference on smart grid communications*. IEEE, 2010. 10.1109/ICCW.2010.5503916.

[BSV16] N. Busom, F. Sebé, and M. Valls. A publicly verifiable counter-based loyalty system. In *Proceedings of the XIV Reunión Española sobre Criptología y Seguridad de la Información*, pages 18–23, 2016. https://goo.gl/DlQmvR.

[CEL+07] L. Chen, A.N. Escalante, H. Löhr, M. Manulis, and A. Sadeghi. A privacy-protecting multi-coupon scheme with stronger protection against splitting. In *Proceedings of financial cryptography and data security*, volume 4886 of *FC'07*, pages 29–44. Springer-Verlag, Berlin, Heidelberg, 2007. 10.1007/978-3-540-77366-5_4.

[CES+05] L. Chen, M. Enzmann, A. Sadeghi, M. Schneider, and M. Steiner. A privacy-protecting coupon system. In *Proceedings of financial cryptography and data security*, FC'05, pages 93–108. Springer-Verlag, Berlin, Heidelberg, 2005. 10.1007/11507840_12.

[CGH06] S. Canard, A. Gouget, and E. Hufschmitt. A handy multi-coupon system. In *Proceedings of applied cryptography and network security*, ACNS'06, pages 66–81. Springer-Verlag, Berlin, Heidelberg, 2006. 10.1007/11767480_5.

[CGHH10] J. Camenisch, T. Groß, P. Hladky, and C. Hoertnagl. Privacy-friendly incentives and their application to wikipedia. In *Policies and research in identity management*, IFIP Advances in information and communication

technology, vol. 343, pages 113–129. Springer-Verlag, Berlin, Heidelberg, 2010. 978-3-642-17302-8, 10.1007/978-3-642-17303-5_9.

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in cryptology — EUROCRYPT'97*, pages 103–118. Springer-Verlag, Berlin, Heidelberg, 1997. 978-3-540-69053-5, 10.1007/3-540-69053-0_9.

[Cha83] D. Chaum. Blind signatures for untraceable payments. In *Advances in cryptology: proceedings of Crypto 82*, pages 199–203. Springer US, 1983. 978-1-4757-0602-4, 10.1007/978-1-4757-0602-4_18.

[Cha89] D. Chaum. Privacy protected payments: unconditional payer and/or payee untraceability. In *Proceedings of the IFIP*, SMART CARD 2000: The future of IC Cards, pages 69–93. Elsevier, 1989.

[CIF+03] S. Chokhani, Orion Security Solutions Inc., W. Ford, Verisign Inc., R. Sabett, Cooley Godward LLP, C. Merrill, McCarter & English LLP, S. Wu, and Infoliance Inc. Internet X.509 public key infrastructure certificate policy and certification practices framework, 2003. https://goo.gl/dahgma.

[CMT05] C. Castelluccia, E. Mykletun, and G Tsudik. Efficient aggregation of encrypted data in wireless sensor networks. In *Proceedings of the 2nd annual international conference on mobile and ubiquitous systems: networking and services*, pages 109–117. IEEE, 2005. 10.1109/MOBIQUITOUS.2005.25.

[Col16] Colak, I. and Sagiroglu, S. and Fulli, G. and Yesilbudak, M. and Covrig, C. A survey on the critical issues in smart grid technologies. *Renewable and sustainable energy reviews*, 54:396–405, 2016. 1364-0321, 10.1016/j.rser.2015.10.036.

[CP93] D. Chaum and T.P. Pedersen. Wallet databases with observers. In *Proceedings of advances in cryptology*, CRYPTO'92, pages 89–105. Springer-Verlag, Berlin, Heidelberg, 1993. 10.1007/3-540-48071-4_7.

[DC17] Q. Ding and S. Cao. RECT: a cloud-based learning tool for graduate goftware engineering practice courses with remote tutor support. *IEEE Access*, 5:1–10, 2017. 2169-3536, 10.1109/ACCESS.2017.2664070.

[Dev15] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 6.6)*, 2015. `http://www.sagemath.org`, 10.5281/zenodo.17093.

[DF90] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In *Proceedings of advances in cryptology*, CRYPTO'89, pages 307–315. Springer-Verlag, New York, 1990. 10.1007/0-387-34805-0_28.

[DFKZB13] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin. Smart meter aggregation via secret-sharing. In *Proceedings of the 1st ACM workshop on smart energy grid security*, SEGS'13, pages 75–80, 2013. 10.1145/2516930.2516944.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE transactions on information theory*, 22(6):644–654, 1976. 0018-9448, 10.1109/TIT.1976.1055638.

[Dim14] T. Dimitriou. Secure and scalable aggregation in the smart grid. In *Proceedings of the 6th international conference on new technologies, mobility and security*, NTMS'14, pages 1–5. IEEE, 2014. 10.1109/NTMS.2014.6814048.

[Dou02] J.R. Douceur. The sybil attack. In *Peer-to-peer systems*, IPTPS'02, pages 251–260. Springer-Verlag, Berlin, Heidelberg, 2002. 3-540-44179-4, 10.1007/3-540-45748-8_24.

[EFS04] M. Enzmann, M. Fischlin, and M. Schneider. A privacy-friendly loyalty system based on discrete logarithms over elliptic curves. In *Proceedings of financial cryptography*, FC'04, pages 24–38. Springer-Verlag, Berlin, Heidelberg, 2004. 10.1007/978-3-540-27809-2_4.

[EK10] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Proceedings of the 1st IEEE international conference on smart grid communications*, pages 238–243. IEEE, 2010. 10.1109/SMARTGRID.2010.5622050.

[Ele17] Electronics maker. Is 2017 the year of smart meter?, 2017. https://goo.gl/snWScz.

[ElG85] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology — CRYPTO'84*, pages 10–18. Springer-Verlag, Berlin, Heidelberg, 1985. 978-3-540-15658-1, 10.1007/3-540-39568-7_2.

[ES05] M. Enzmann and M. Schneider. Improving customer retention in e-Commerce through a secure and privacy-enhanced loyalty system. *Information systems frontiers*, 7(4):359–370, 2005. 1387-3326, 10.1007/s10796-005-4808-2.

[Esc07] Escalante, A.N. and Löhr, H. and Sadeghi, A. A non-sequential unsplittable privacy-protecting multi-coupon scheme. In *Jahrestagung der Gesellschaft für Informatik*, volume 110 of *INFORMATIK'07*, pages 184–188. GI, 2007. https://goo.gl/JGBs4w.

[Eur17] European Comission. Smart grids and meters, 2017. https://goo.gl/nWRWOa.

[FB13] S. Finster and I. Baumgart. Pseudonymous smart metering without a trusted third party. In *Proceedings of the 12th IEEE international conference on trust, security and privacy in computing and communications*, pages 1723–1728, 2013. 10.1109/TrustCom.2013.234.

[Fel87] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th annual symposium on foundations of computer science*, SFCS'87, pages 427–438. IEEE, 1987. 10.1109/SFCS.1987.4.

[FG07] C. Fontaine and F. Galand. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, 2007, 2007. 1687-417X, 10.1155/2007/13801.

[FG10] F.R. Farmer and B. Glass. *Building web reputation systems*. Yahoo! Press, 2010.

[FRS17] S. Falk, A. Römmele, and M. Silverman. The promise of digital government. In *Digital government: leveraging innovation to improve public sector performance and outcomes for citizens*, pages 3–23. Springer international publishing, 2017. 978-3-319-38795-6, 10.1007/978-3-319-38795-6_1.

[Gar17] Inc. Gartner. Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016, 2017. https://goo.gl/E0YOsB.

[GJ11] F.D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Security and trust management: STM 6th international workshop*, pages 226–238. Springer-Verlag, Berlin, Heidelberg, 2011. 978-3-642-22444-7, 10.1007/978-3-642-22444-7_15.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the 17th annual ACM symposium on theory of computing*, STOC'85, pages 291–304. ACM, 1985. 10.1145/22145.22178.

[GMSP+13] F. Gómez Mármol, C. Sorge, R. Petrlic, O. Ugus, D. Westhoff, and G. Martínez Pérez. Privacy-enhanced architecture for smart metering. *International journal of information security*, 12(2):67–82, 2013. 1615-5270, 10.1007/s10207-012-0181-6.

[HBC15] F. Hendrikx, K. Bubendorfer, and R. Chard. Reputation systems: a survey and taxonomy. *Journal of parallel and distributed computing*, 75:184–197, 2015. 0743-7315, 10.1016/j.jpdc.2014.08.004.

[HMV03] D. Hankerson, A.J. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer-Verlag, New York, 2003. 038795273X, 10.1007/b97644.

[HMV04] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer-Verlag, New York, 2004. 10.1007/b97644.

[HR17] R.D. Hisrich and V. Ramadani. E-commerce challenges and entrepreneurial manager. In *Effective entrepreneurial management: strategy, planning, risk management, and organization*, pages 159–178. Springer international publishing, 2017. 978-3-319-50467-4, 10.1007/978-3-319-50467-4_9.

[Ibe14] Iberdrola. Prices and capacity power 2014, 2014. https://goo.gl/zf7cHI.

[IDHFGPC11] A.P. Isern-Deya, M.F. Hinarejos, J.-L. Ferrer-Gomila, and M. Payeras-Capella. A secure multicoupon solution for multi-merchant scenarios. In *Proceedings of the 10th International Conference on Trust, Security and*

Privacy in Computing and Communications, TrusCom'11, pages 655–663. IEEE, 2011. 10.1109/TrustCom.2011.84.

[JK12] M. Jawurek and F. Kerschbaum. Fault-tolerant privacy-preserving statistics. In *Privacy enhancing technologies: PETS 12th International Symposium*, pages 221–238. Springer-Verlag, Berlin, Heidelberg, 2012. 978-3-642-31680-7, doi 10.1007/978-3-642-31680-7_12.

[JSl] Javascript crypto libraries. https://goo.gl/4WJ4uo.

[KDK11] K. Kursawe, G. Danezis, and M. Kohlweiss. Privacy-friendly aggregation for the smart-grid. In *Privacy enhancing technologies: PETS 11th international symposium*, pages 175–191. Springer-Verlag, Berlin, Heidelberg, 2011. 978-3-642-22263-4, 10.1007/978-3-642-22263-4_10.

[Ker09] F. Kerschbaum. A verifiable, centralized, coercion-free reputation system. In *Proceedings of the 8th ACM workshop on privacy in the electronic society*, WPES'09, pages 61–70. ACM, 2009. 10.1145/1655188.1655197.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48:203–209, 1987. 10.1090/S0025-5718-1987-0866109-5.

[KPS15] A. Kokoschka, R. Petrlic, and C. Sorge. A reputation system supporting unlinkable, yet authorized expert ratings. In *Proceedings of the 30th ACM/SIGAPP symposium on applied computing*, SAC'15, pages 2320–2327. ACM, 2015. 10.1145/2695664.2695892.

[LLL10] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. In *Proceedings of the 1st IEEE international conference on smart grid communications*, pages 327–332. IEEE, 2010. 10.1109/SMARTGRID.2010.5622064.

[LLL+12] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE transactions on parallel and distributed systems*, 23(9):1621–1631, 2012. 10.1109/TPDS.2012.86.

[McE14] A. McEachern. A history of loyalty programs, and how they have changed, 2014. https://goo.gl/OQrUj8.

[Mil86] V.S. Miller. Use of elliptic curves in cryptography. In *Proceedings of advances in cryptology*, CRYPTO'85, pages 417–426. Springer-Verlag, Berlin, Heidelberg, 1986. 10.1007/3-540-39799-X_31.

[MLV07] G. D. Magoulas, G. Lepouras, and C. Vassilakis. Virtual reality in the e-Society. *Virtual Reality*, 11(2):71–73, 2007. 1359-4338, 10.1007/s10055-006-0064-0.

[MNDA+17] M. Moretti, S. Njakou Djomo, H. Azadi, K. May, K. De Vos, S. Van Passel, and N. Witters. A systematic review of environmental and economic impacts of smart grids. *Renewable and sustainable energy reviews*, 68, Part 2:888–898, 2017. 1364-0321, 10.1016/j.rser.2016.03.039.

[MOV91] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the 23rd annual ACM symposium on theory of computing*, STOC'91, pages 80–89. ACM, 1991. 10.1145/103418.103434.

[MVVO96] A.J. Menezes, S.A. Vanstone, and P.C. Van Oorschot. *Handbook of applied cryptography*. CRC Press, 1996. https://goo.gl/eOb2hP.

[Ngu06] L. Nguyen. Privacy-protecting coupon system revisited. In *Proceedings of financial cryptography and data security*, volume 4107 of *FC'06*, pages 266–280. Springer-Verlag, Berlin, Heidelberg, 2006. 10.1007/11889663_22.

[NMVI09] R. Nickerson, J. Muntermann, U. Varshney, and H. Isaac. Taxonomy development in information systems: developing a taxonomy of mobile applications, 2009. https://goo.gl/ywltfn.

[NS08] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *Proceedings of the 2008 IEEE symposium on security and privacy*, SP'08, pages 111–125. IEEE, 2008. 10.1109/SP.2008.33.

[OIV+14] A. Opromolla, A. Ingrosso, V. Volpi, M. Pazzola, and C. Medaglia. A user-centered approach in designing NFC couponing platform: the case study of CMM applications. In *HCI in Business*, Lecture Notes in Computer Science, vol. 8527, pages 360–370. Springer-Verlag, Cham, 2014. 10.1007/978-3-319-07293-7_35.

[OK04] W. Ogata and K. Kurosawa. Oblivious keyword search. *Journal of complexity*, 20(2-3):356–371, 2004. 10.1016/j.jco.2003.08.023.

[Pai99] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the 17th international conference on theory and application of cryptographic techniques*, EUROCRYPT'99, pages 223–238. Springer-Verlag, Berlin, Heidelberg, 1999. https://goo.gl/6O1mBi.

[Ped91] T.P. Pedersen. A threshold cryptosystem without a trusted party. In *Advances in cryptology — EUROCRYPT'91*, pages 522–526. Springer-Verlag, Berlin, Heidelberg, 1991. 978-3-540-46416-7, 10.1007/3-540-46416-6_47.

[Pet10] R. Petrlic. A privacy-preserving concept for smart grids. In *Proceedings of Sicherheit in vernetzten Systemen: 18 DFN Workshop*, pages B1–B14, 2010.

[PLS14] R. Petrlic, S. Lutters, and C. Sorge. Privacy-preserving reputation management. In *Poceedings of 29th annual ACM symposium on applied computing*, SAC'14, pages 1712–1718, 2014. 10.1145/2554850.2554881.

[PP16] J. Pelzl and C. Paar. Digitale Signaturen. In *Kryptografie verständlich: ein Lehrbuch für Studierende und Anwender*, pages 297–333. Springer-Verlag, Berlin, Heidelberg, 2016. 10.1007/978-3-662-49297-0_10.

[RKZF00] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Communications of the ACM*, 43(12):45–48, 2000. 0001-0782, 10.1145/355112.355122.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. 0001-0782, 10.1145/359340.359342.

[SBHB16] A. Schaub, R. Bazin, O. Hasan, and L. Brunie. A trustless privacy-preserving reputation system. In *IFIP advances in information and communication technology, vol 471*, SEC'16, pages 398–411. Springer-Verlag, Cham, 2016. 978-3-319-33630-5, 10.1007/978-3-319-33630-5_27.

[Sch90] C.P. Schnorr. Efficient identification and signatures for smart cards. In *Advances in cryptology — EUROCRYPT'89*, pages 688–689. Springer-Verlag, Berlin, Heidelberg, 1990. 978-3-540-46885-1, 10.1007/3-540-46885-4_68.

[SG11] G. Shani and A. Gunawardana. Evaluating recommendation systems. In *Recommender systems handbook*, pages 257–297. Springer-Verlag, US, 2011. 978-0-387-85819-7, 10.1007/978-0-387-85820-3_8.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. 10.1145/359168.359176.

[Shi00] R. Shirey. IETF RFC 2828: Internet security glossary. Technical report, RFC, 2000. https://goo.gl/7pKBSg.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 2nd edition edition, 2009. 978-0387094939, 10.1007/978-0-387-09494-6.

[SS98] J.H. Silverman and J. Suzuki. Elliptic curve discrete logarithms and the index calculus. In *Proceedings of advances in cryptology*, ASIACRYPT'98, pages 110–125. Springer-Verlag, Berlin, Heidelberg, 1998. 10.1007/3-540-49649-1_10.

[Ste06] S. Steinbrecher. Design options for privacy-respecting reputation systems within centralised internet communities. In *Security and privacy in dynamic environments*, volume 201 of *IFIP international federation for information processing*, pages 123–134. Springer-Verlag, Boston, 2006. 0-387-33405-X, 10.1007/0-387-33406-8_11.

[TRP13] E. Toufaily, L. Ricard, and J. Perrien. Customer loyalty to a commercial website: Descriptive meta-analysis of the empirical literature and proposal of an integrative model. *Journal of Business Research*, 66(9):1436–1447, 2013. 10.1016/j.jbusres.2012.05.011.

[Vos04] M. Voss. Privacy preserving online reputation systems. In *Information security management, education and privacy*, pages 249–264. Springer-Verlag, Boston, 2004. 978-1-4020-8144-6, 10.1007/1-4020-8145-6_20.

[VSA+15] J. Vilaplana, F. Solsona, F. Abella, J. Cuadrado, I. Teixidó, J. Mateo, and J. Rius. H-PC: a cloud computing tool for supervising hypertensive patients. *The Journal of Supercomputing*, 71(2):591–612, 2015. 0920-8542, 10.1007/s11227-014-1312-9.

[VUWS12] B. Vetter, O. Ugus, D. Westhoff, and C. Sorge. Homomorphic primitives for a privacy-friendly smart metering architecture. In *Proceedings of the international conference on security and cryptography*, SECRYPT'12, pages 102–112, 2012. https://goo.gl/yX2JCA.

[Wan17] Wang, J. and Hui, L. and Yiu, S.M. and Wang, E. and Fang, J. A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities. *Pervasive and Mobile Computing*, page (In press), 2017. 1574-1192, 10.1016/j.pmcj.2017.04.005.

[WLT00] A.M. Wibowo, K.Y. Lam, and G.S.H. Tan. Loyalty program scheme for anonymous payment systems. In *Electronic commerce and web technologies*, EC-Web'02, pages 253–265. Springer-Verlag, Berlin, Heidelberg, 2000. 10.1007/3-540-44463-7_22.

[YK11] S.K. Yadav and M. Kumar. On certain attacks and privacy - protecting coupon system: a model. *International journal of theoretical and applied science*, 3(2):79–87, 2011. 0975-1718, https://goo.gl/i9T8qT.